OBSERVACIBER

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS

ESTUDIO SOBRE PERCEPCIÓN
Y NIVEL DE CONFIANZA EN ESPAÑA

Edición Diciembre 2021

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi | incibe_ | OBSERVACIBER

ÍNDICE

1. Introducción al estudio
2. Módulo I: Servicios usados en Internet
3. Módulo II: Medidas y hábitos de seguridad en Internet
4. Módulo III: Hábitos de comportamiento en la navegación y uso de Internet
5. Módulo IV: Incidencias de seguridad
6. Módulo V: Fraude
7. Módulo VI: Seguridad en Wi-Fi
8. Módulo VII: Opinión
9. Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton
10. Alcance del estudio

Introducción al estudio

Introducción al estudio

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) de Red.es, ha diseñado y promovido el:

Estudio sobre la Ciberseguridad y Confianza en los hogares españoles

Esta investigación es referente en el diagnóstico sobre el estado de la ciberseguridad en los hogares digitales españoles, analizando la adopción de medidas de seguridad y el nivel de incidencia de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en la Sociedad de la Información.

Los datos presentados en este informe han sido extraídos siguiendo diferentes metodologías:

- Dato declarado: Obtenido de las encuestas online realizadas a los 3.711 hogares que han conformado la muestra del estudio.
- Dato real: Para ello se utiliza el *software* **Pinkerton** desarrollado por Hispasec Sistemas, que analiza los dispositivos recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas. **Pinkerton** también detecta la presencia de *malware* en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 70 motores antivirus. Los datos así extraídos se representan en el presente informe con la siguiente etiqueta:

Los datos reflejados en **este informe abarcan el análisis desde enero hasta junio de 2021**.

Introducción al estudio

El actual estudio recoge información concerniente a datos presentados en estudios sobre la ciberseguridad y confianza en los hogares españoles realizados con anterioridad.

El objetivo es poder contrastar dicha información con la obtenida en el presente estudio, y de este modo determinar la evolución experimentada en el ámbito de la ciberseguridad y confianza digital.

Para designar a cada estudio se han utilizado las nomenclaturas que se exponen a continuación:

- **1S20**, estudio realizado en el primer semestre de 2020 (enero - junio).
- **2S20**, estudio realizado en el segundo semestre de 2020 (julio – diciembre).
- **1S21**, estudio realizado en el primer semestre de 2021 (enero - junio).

Introducción al estudio

El **objetivo general** de este estudio es hacer un **análisis del estado real** de la **ciberseguridad y confianza digital** entre los usuarios españoles de Internet y, al mismo tiempo, contrastar el nivel real de incidentes que sufren los equipos y dispositivos móviles con las percepciones de los usuarios además de mostrar la evolución temporal de estos indicadores.

Además se trata de **impulsar** el **conocimiento especializado y útil** en materia de **ciberseguridad y privacidad**, para mejorar la implantación de medidas por parte de los usuarios.

Así mismo se pretende reforzar la **adopción de políticas y medidas** por parte de la Administración, orientando iniciativas y políticas públicas tanto en la generación de confianza en la Sociedad de la Información, como en la mejora individual de la seguridad, sustentadas en una percepción realista de los beneficios y riesgos de las mismas.

Introducción al estudio

Medidas de seguridad[1]

Son programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentren en este. Estas herramientas y acciones pueden ser realizadas con la intervención directa del usuario **(automatizables y no automatizables)** y pueden ser también medidas anteriores o posteriores a que ocurra la incidencia de seguridad **(proactivas, reactivas o ambas).**

Medidas automatizables

Son aquellas medidas de **carácter pasivo** que, por lo general, no requieren de **ninguna acción por parte del usuario**, o cuya configuración permite una puesta en marcha automática.

Medidas no automatizables

Son aquellas medidas de **carácter activo** que, por lo general, **sí requieren una actuación específica por parte del usuario** para su correcto funcionamiento.

Medidas proactivas

Son aquellas medidas utilizadas para **prevenir y evitar**, en la medida de lo posible, la ocurrencia de incidencias de seguridad y minimizar las posibles **amenazas desconocidas y conocidas**.

Medidas reactivas

Son aquellas medidas que son utilizadas para **subsanar** una incidencia de seguridad, es decir, son las medidas que se utilizan para eliminar **amenazas conocidas y /o incidencias ocurridas**.

[1] Existen medidas de seguridad que, por su condición, se pueden clasificar en varias categorías, tal es el caso de los programas antivirus y sus actualizaciones, o las del sistema operativo. Un programa antivirus, por su naturaleza, puede detectar tanto las amenazas existentes en el equipo como aquellas que intenten introducirse en él.

Introducción al estudio

	Medidas automatizables	Medidas no automatizables
Proactivas	• **Cortafuegos o firewall**	• **Contraseñas** • **Copias de seguridad de archivos** • **Partición del disco duro** • **Certificados digitales de firma electrónica** • **Utilización habitual de permisos reducidos** • **DNI electrónico** • **Cifrado de documentos o datos** • **Uso de máquinas virtuales**
Proactivas y reactivas	• **Programa antivirus** • **Actualizaciones del sistema operativo y programas** • **Actualizaciones del antivirus**	
Reactivas	• **Plugins para el navegador** • **Programas de bloqueo de ventanas emergentes** • **Programas de bloqueo de banners** • **Programas anti-spam** • **Programas anti-fraude**	• **Eliminación de archivos temporales o cookies**

Introducción al estudio

Se denomina *malware* a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un PC/portátil o dispositivo móvil (*tablet*, *smartphone*, relojes inteligentes, etc.) sin el consentimiento del propietario. Comúnmente se conocen como virus, en realidad se trata de un término más amplio que engloba otras tipologías.

Troyanos o caballos de Troya. *Bankers* o troyanos bancarios, *Backdoors* o puertas traseras, *Keyloggers* o capturadores de pulsaciones, *Dialers* o marcadores telefónicos, *Rogueware*

***Adware* o *software* publicitario**

Herramientas de intrusión

Virus

Archivos sospechosos detectados heurísticamente. Técnica empleada por los antivirus para reconocer códigos maliciosos que no se encuentran en la base de datos de virus del antivirus

***Spyware* o programas espía**

Gusano o *worm*

Otros. *Exploit, Rootkits, Scripts, Lockers* o *Scareware*, *Jokes* o bromas

Mas información: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

Introducción al estudio

Para determinar el nivel de riesgo[3] de los equipos analizados, se establece la peligrosidad del *malware* detectado en función de las posibles consecuencias sufridas. La clasificación se realiza en base a los siguientes criterios:

- **Peligrosidad alta**: se incluyen en esta categoría los especímenes que, potencialmente: permiten el acceso remoto por parte de un atacante al sistema víctima; pueden suponer un perjuicio económico para el usuario; facilitan la captura de información confidencial o sensible de la víctima; se emplean como pasarelas para atacar otros equipos (pudiendo acarrear consecuencias legales para la víctima); o minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

- **Peligrosidad media**: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema: no perjudican de forma notoria su rendimiento; abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; o facilitan la captura de información no sensible de la víctima (por ejemplo, patrones de navegación para crear perfiles de publicidad dirigida, etc.).

- **Peligrosidad baja**: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, etc.). En la mayoría de los casos son herramientas instaladas por el usuario de forma intencionada, para listar y matar procesos, o conectarse remotamente a su equipo, etc. Por otra parte, también se consideran especímenes de baja peligrosidad los programas "broma" (por ejemplo aquellos que despliegan una ventana que se va moviendo y resulta imposible cerrarla con el ratón) y los virus exclusivos para plataformas móviles, ya que estos no son capaces de ejecutarse sobre los equipos de los usuarios.

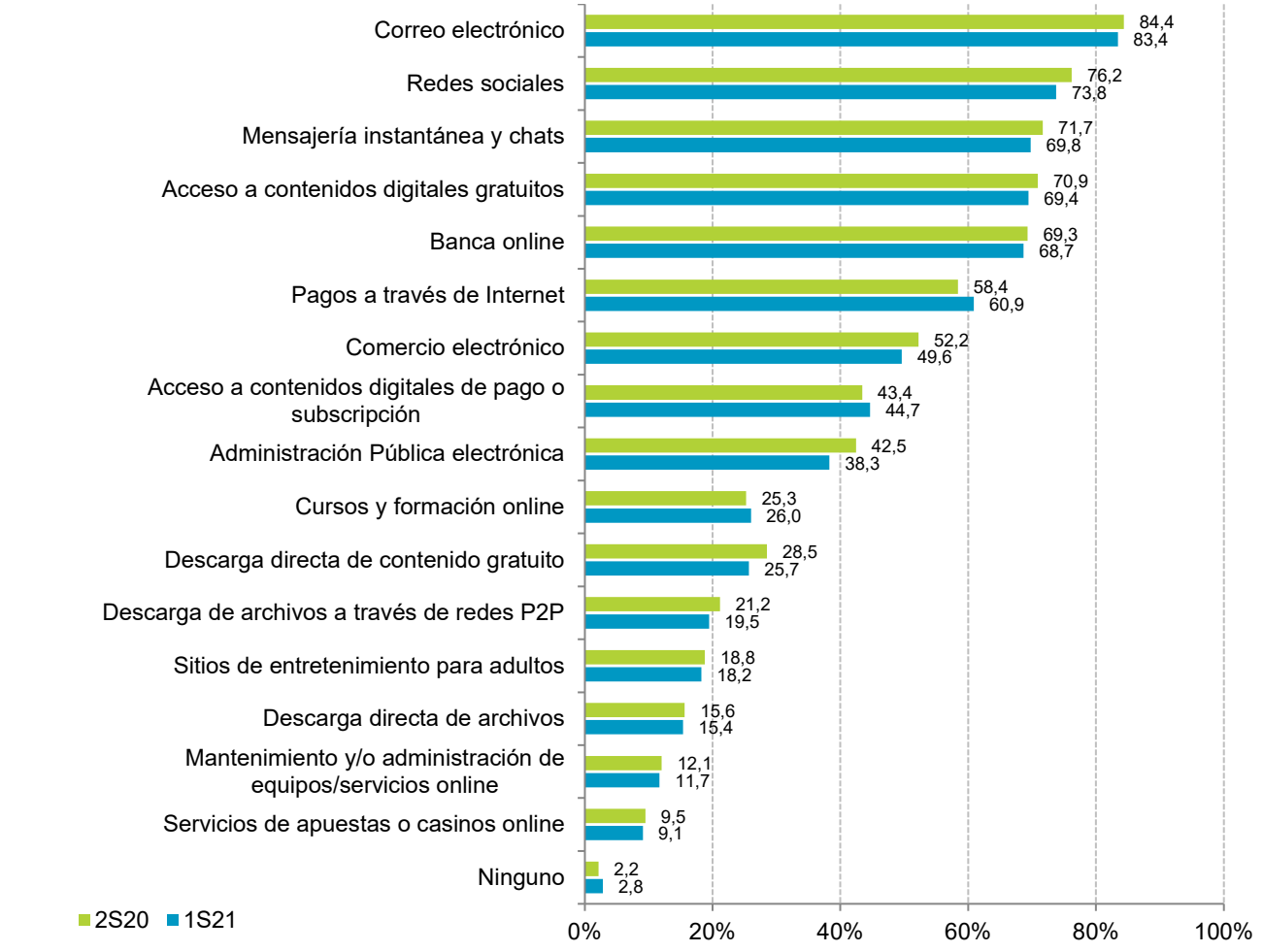
[3] Se establece como el nivel de riesgo de cada equipo el de mayor nivel de entre el *malware* que aloje. Es decir, un equipo en el que se detecte un *software* malicioso de peligrosidad alta y otro de peligrosidad media, siempre será incluido en el grupo de equipos con un nivel de riesgo alto.

Módulo I:
Servicios usados en Internet

Módulo I: Servicios usados en Internet

Servicios ofrecidos por Internet que han sido utilizados por el usuario en el último semestre

En el último semestre y según declaraciones de los usuarios, ha descendido levemente el uso de todos los servicios online, a excepción de los pagos a través de internet 60,9% (+2,5 puntos porcentuales), el acceso a contenidos digitales de pago o subscripción 44,7% (+1,3 p.p.) y los cursos y formación online 26,0% (+0,7 p.p.).



Base: Total usuarios

Módulo I: Servicios usados en Internet

Motivos de no utilización de los servicios ofrecidos por Internet

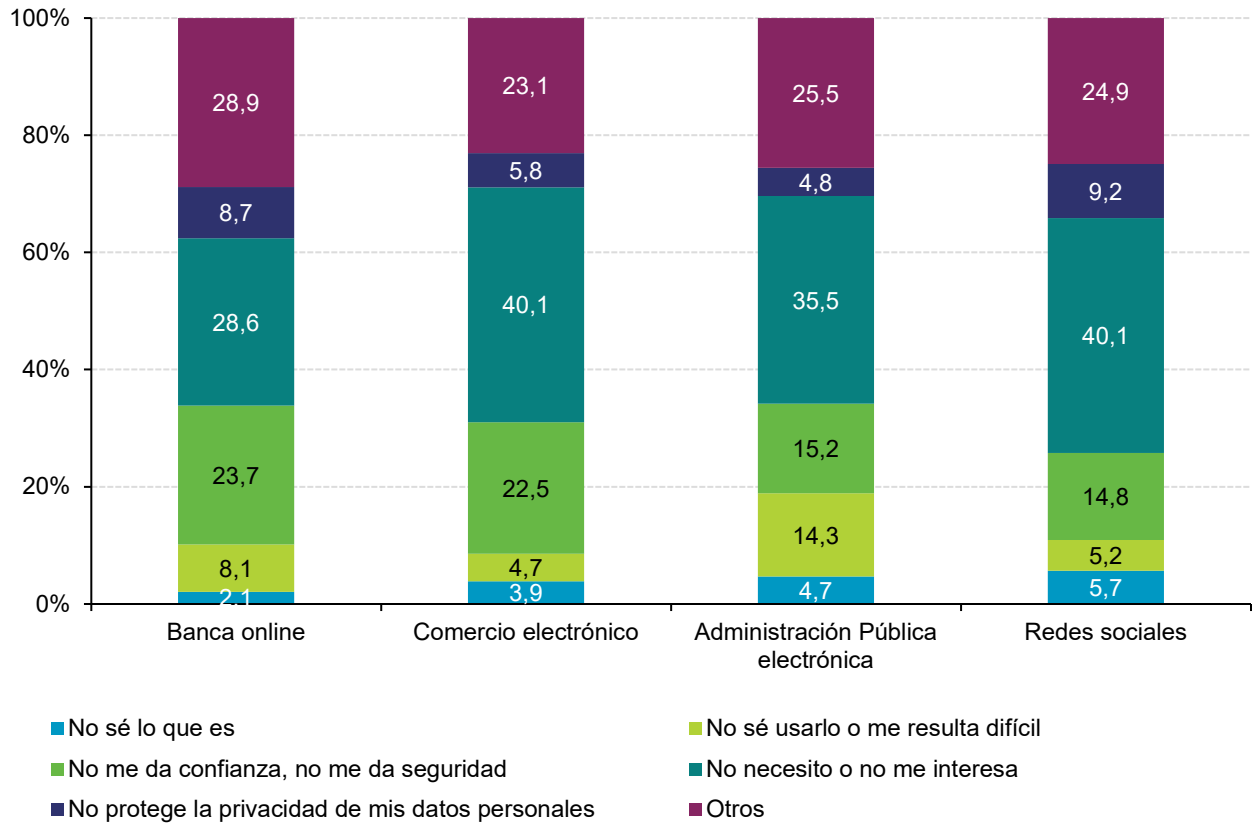
La falta de privacidad en redes sociales es importante para el 9,2% de los usuarios encuestados, que alegan no usarlas por dicho motivo. Por otra parte, el 40,1% de los usuarios que no utilizan estas redes sociales, indican que no les son necesarias o no les interesa.

También destaca que el 14,3% de los usuarios no saben usar o les resulta difícil, el uso de la administración pública electrónica.

El servicio más conocido por los panelistas es el de la banca online, únicamente un 2,1% de los usuarios que no lo utilizan, declara que es por desconocimiento.

¿Sabes que puedes configurar las opciones de privacidad de las principales redes sociales y aplicaciones de mensajería instantánea? Guía de privacidad y seguridad en Internet:

✓ *https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet*



Base: Usuarios que no utilizan alguno de los servicios

Módulo II:
Medidas y hábitos de seguridad en Internet

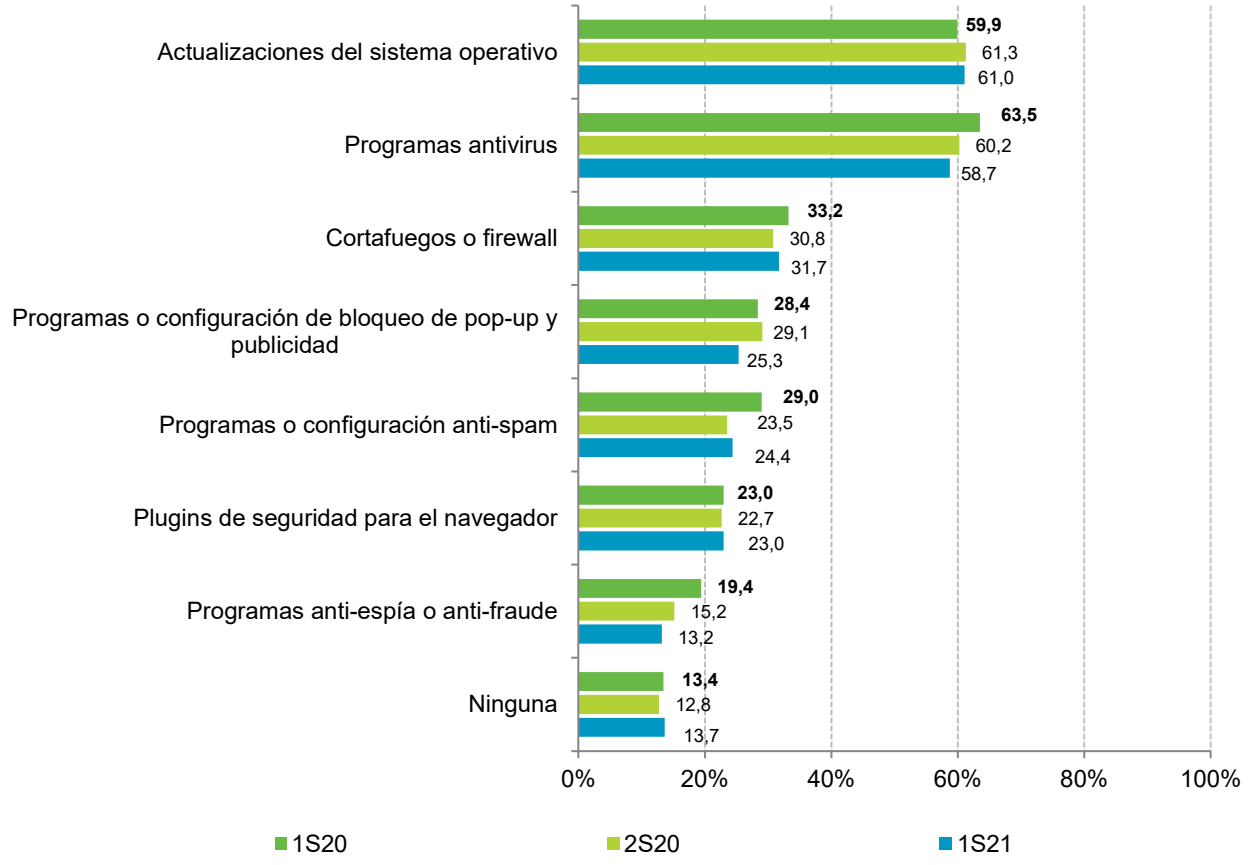
Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad automatizables en el ordenador del hogar

A excepción del uso del cortafuegos o firewall 31,7% y el uso de programas anti-spam 24,4%, el uso de medidas automatizables en el ordenador del hogar, ha disminuido nuevamente de manera generalizada. Conforme a las declaraciones de los panelistas se observa, por tercer semestre consecutivo, un descenso en el uso de los programas antivirus (-1,5 puntos porcentuales respecto a la oleada anterior).

La funcionalidad de los programas antivirus no se limita únicamente a eliminar el malware presente en el equipo informático. Su cometido más importante es prevenir y evitar las infecciones de malware.

Vídeo: Antivirus. ¿cómo nos protegen?
https://youtu.be/f8FWKR7YUq0



Base: Usuarios de PC

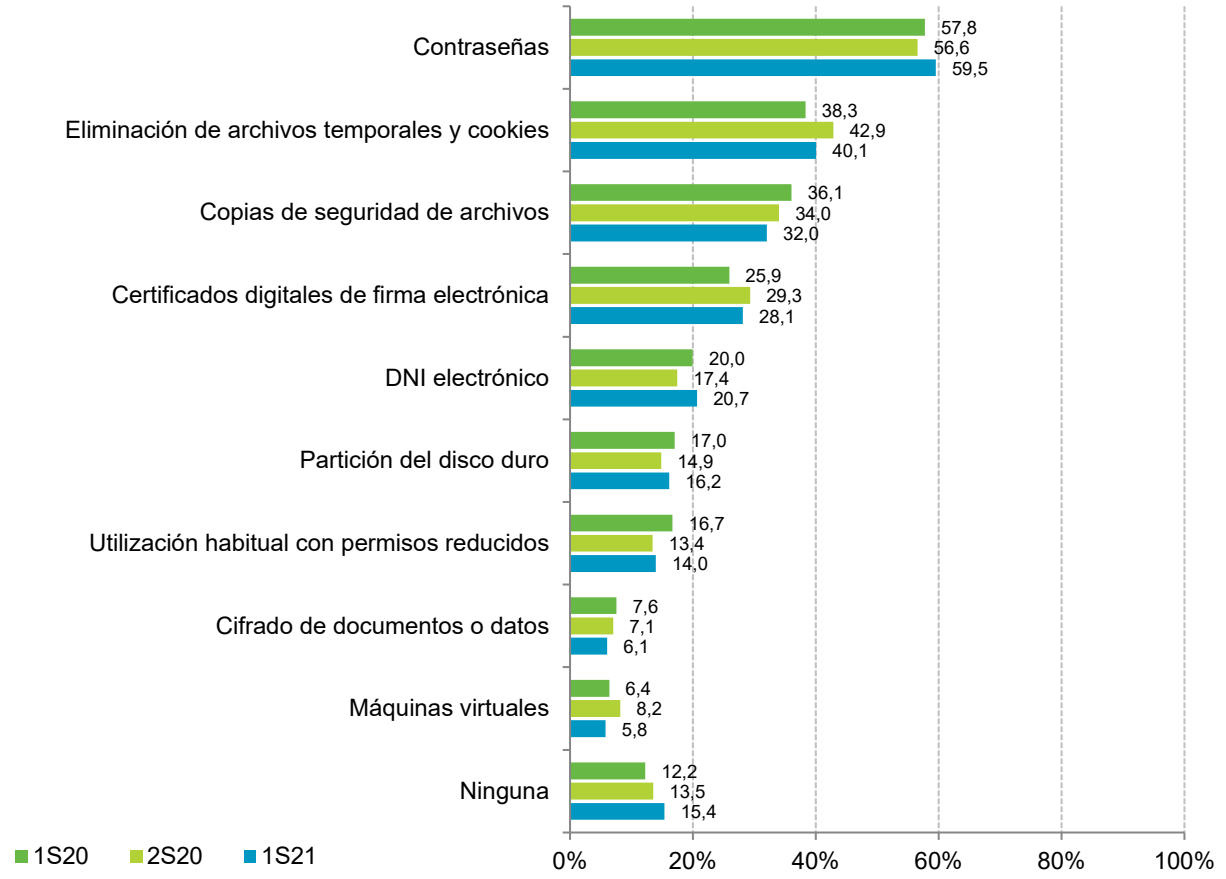
Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad activas o no automatizables en el ordenador del hogar

En el primer semestre de 2021, destaca el uso de contraseñas (59,5%), aumentando casi 3 p.p. respecto al semestre anterior y también el ascenso del uso del DNI electrónico en 3,3 p.p., aunque el uso de certificados digitales siguen siendo una opción más usada por los panelistas frente al DNI electrónico. Se aprecia que el uso de maquinas virtuales, que había crecido en el semestre anterior, vuelve a descender al 5,8%, siendo el menor porcentaje de las tres últimas oleadas.

Es muy importante gestionar correctamente las contraseñas y, además, realizar copias de seguridad de los datos que queremos salvaguardar. Obtén más información sobre cómo realizar estas tareas:

- ✓ ***Contraseñas:*** *https://www.osi.es/es/campanas/contrasenas-seguras*
- ✓ ***Copias de seguridad:*** *https://www.osi.es/es/campanas/copias-cifrado-informacion*



Base: Usuarios de PC

Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad en dispositivos Android

Las medidas de seguridad disponibles en los dispositivos Android, como el uso de pin o patrón de desbloqueo 86,7% , el bloqueo automático del terminal 68,1%, el encriptado de datos 19,0% y el uso de gestores de contraseñas 43,1%, continúan aumentando.

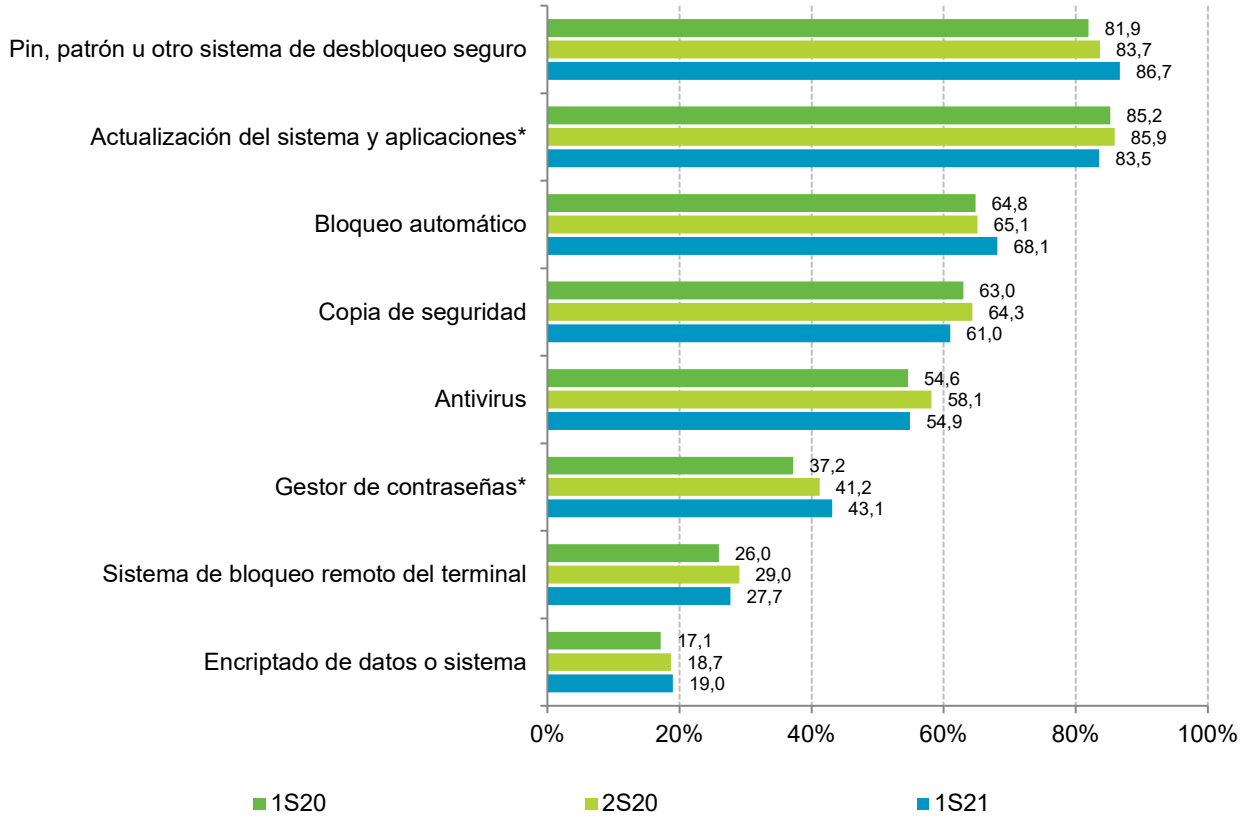
Sin embargo, se aprecia una disminución en el uso de copias de seguridad y antivirus en los terminales de los panelistas.

Nuestros dispositivos móviles contienen muchísima información valiosa para nosotros que, puede ser sustraída si, perdemos nuestro teléfono, nos lo roban o si se infecta por un malware. Obtén más información sobre cómo configurarlos:

https://www.osi.es/es/campanas/dispositivos-moviles

https://www.osi.es/es/campanas/segunda-vida-dispositivos

https://www.osi.es/es/guia-para-configurar-dispositivos-moviles



*nuevas categorías

Base: Usuarios que disponen de dispositivo Android

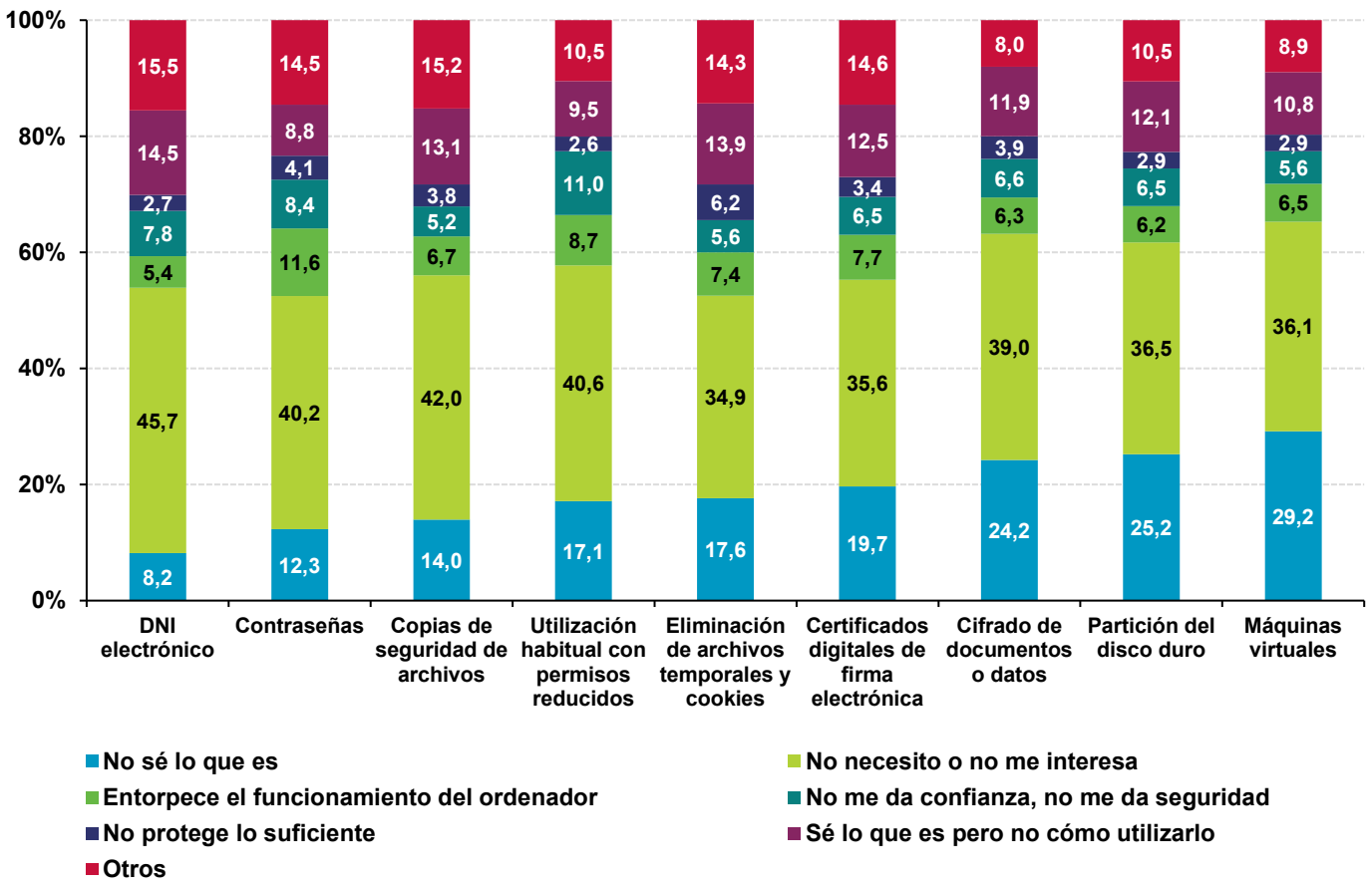
Módulo II: Medidas y hábitos de seguridad en Internet

Motivos de no utilización de medidas de seguridad

El DNI electrónico se encuentra entre las medidas de seguridad más conocidas por los panelistas, donde sólo el 8,2% desconoce lo que es, sin embargo, es la que los usuarios estiman menos necesaria o que tiene menor interés para ellos (45,7%).

Respecto al resto de medidas, cabe destacar que aún, un 12,3% de usuarios no tiene claro qué son las contraseñas o bien, el desconocimiento de aspectos no sólo de seguridad, sino de usabilidad y prevención, como son las copias de seguridad de archivos (14%).

El cifrado permite salvaguardar la privacidad de los datos que manejan los usuarios, ya que en caso de que se produzca una fuga de información, ésta será inaccesible para cualquiera sin la clave de descifrado:
https://www.osi.es/es/actualidad/blog/2019/05/29/cifrado-y-almacenamiento-seguro-de-ficheros-paso-paso



Base: Usuarios de PC que no utilizan alguna de las medidas de seguridad

Módulo III:
Hábitos de comportamiento en la navegación y uso de Internet

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de servicios de banca online o comercio electrónico

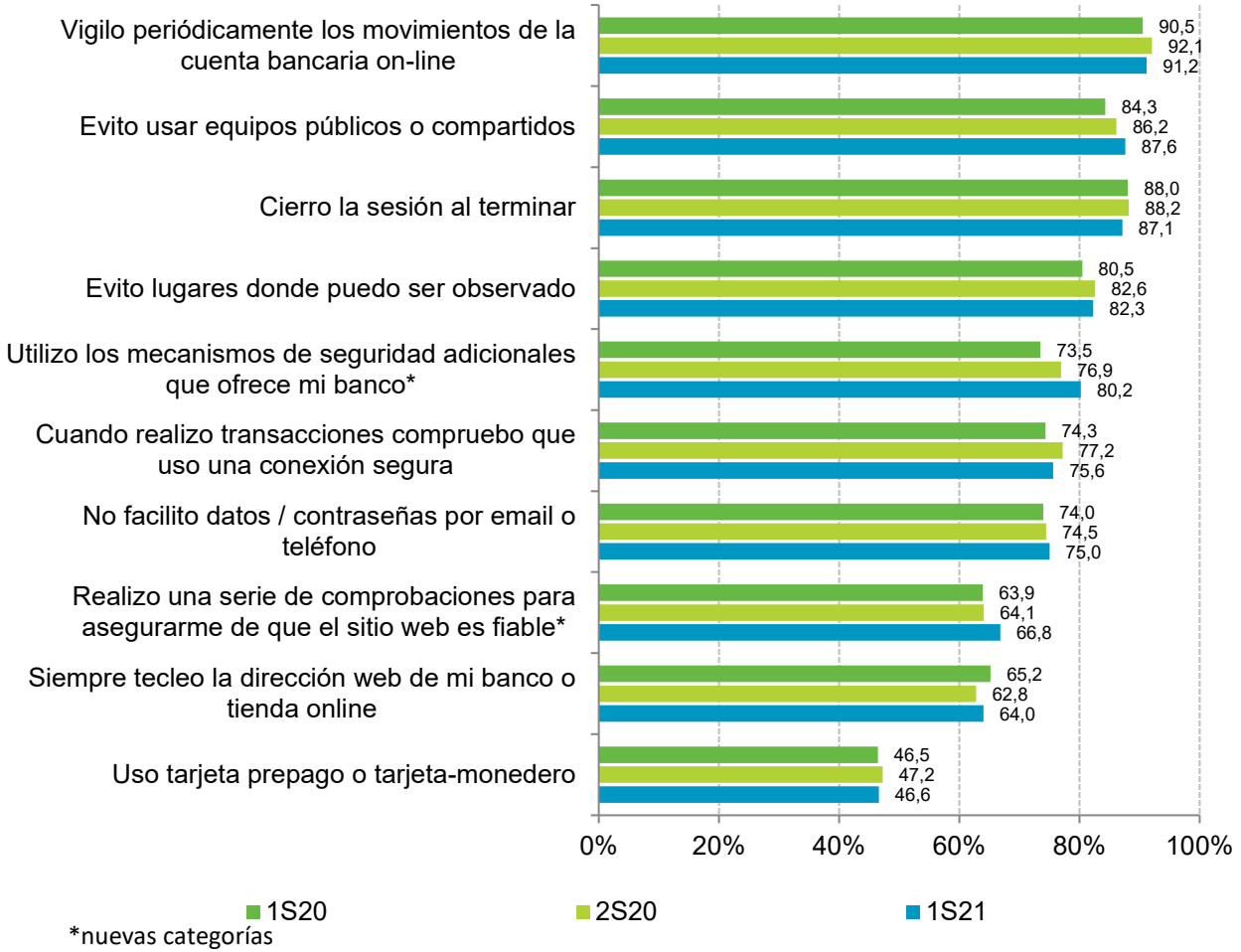
El uso de las nuevas medidas de seguridad de entidades bancarias esta obligando a los usuarios a emplearlas. En esta oleada se puede observar un aumento de 3,3 p.p. con respecto a la anterior.

Mejora de la conducta de los panelistas en relación a compartir datos o contraseñas por internet, realizar comprobaciones para verificar la fiabilidad de la web que visitan y teclear la web del banco en lugar de hacer clic sobre los resultados de búsqueda.

Las entidades bancarias nunca solicitan datos y contraseñas del usuario. Dicha información es confidencial y únicamente debe ser conocida por el usuario y normalmente las entidades bancarias avisan a sus clientes de estas prácticas. La finalidad es evitar fraudes online y/o telefónicos que buscan obtener las credenciales del usuario y conseguir acceso a sus cuentas.

El 1 de enero de 2021 se acabó el plazo para la implantación de la Autenticación Reforzada de Cliente (SCA). Infórmate más sobre la directiva de pago en:

https://www.osi.es/es/actualidad/blog/2019/09/17/informate-lo-que-debes-saber-si-quieres-hacer-pagos-online-partir-de



*nuevas categorías

BASE: Usuarios que utilizan banca online y/o comercio electrónico

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

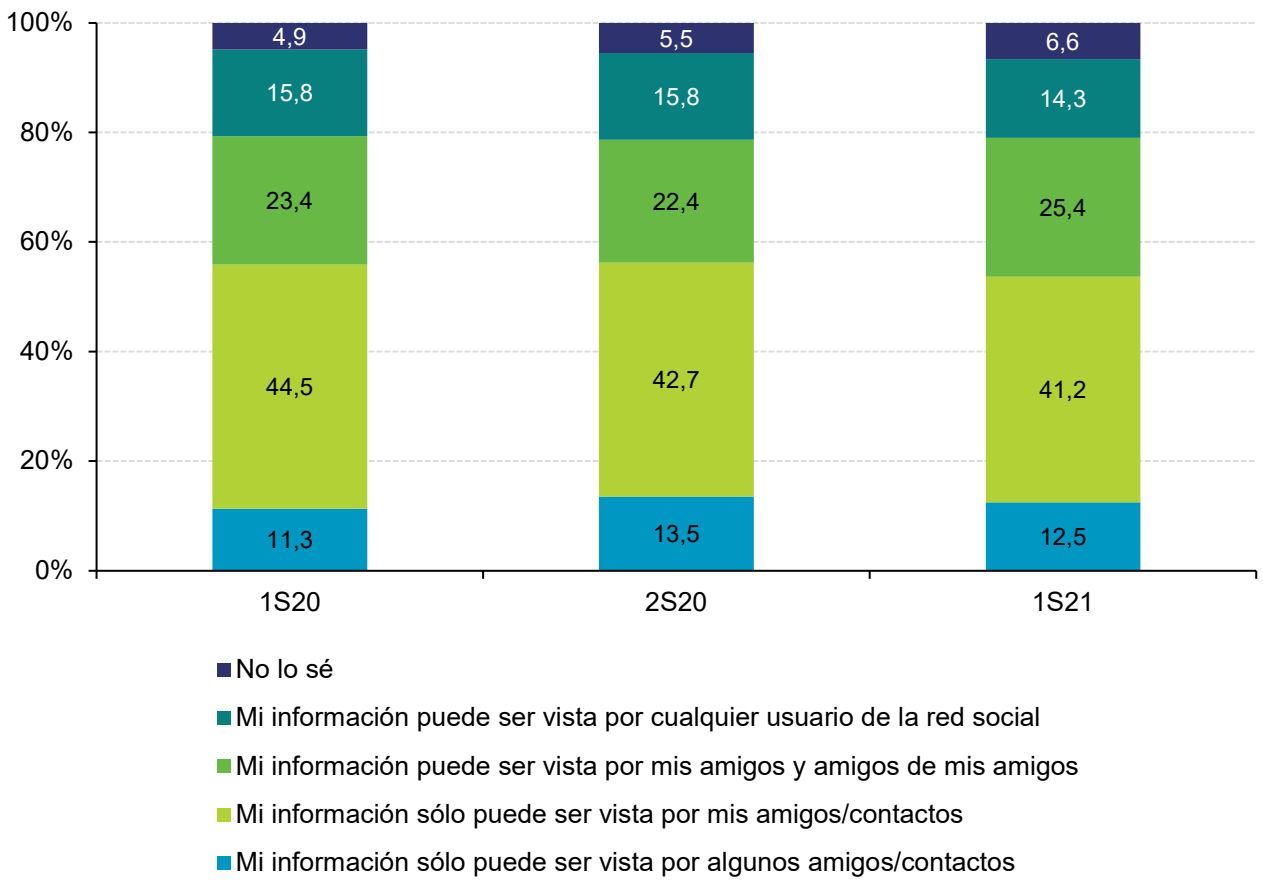
Hábitos de comportamiento en el uso de redes sociales

El uso de las redes sociales para comunicarse con familiares y amigos sigue siendo un medio de comunicación muy utilizado.

El 14,3% de los usuarios manifiesta que la información que comparten en redes sociales es pública y puede verla cualquiera, aunque se puede observar una disminución de un punto porcentual respecto al semestre anterior.

Descubre qué información se almacena en las redes sociales Facebook, Instagram, Twitter y LinkedIn sobre ti y quién puede acceder a ella:

https://www.osi.es/es/actualidad/blog/2020/01/22/descarga-tu-vida-de-las-redes-sociales



BASE: Usuarios de redes sociales

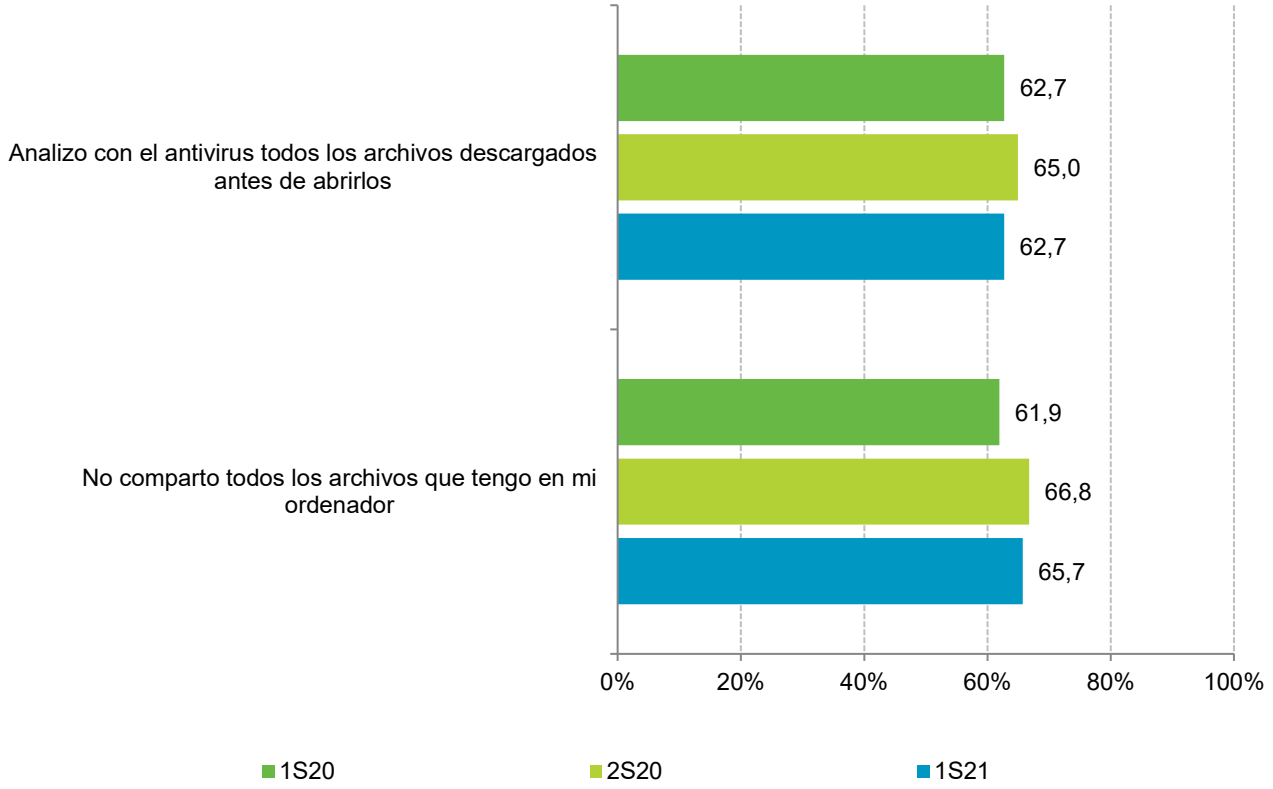
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de redes P2P

Según las declaraciones de los usuarios, el 62,7% analiza los archivos descargados a través de las redes P2P antes de abrirlos. Este hábito de comportamiento ha descendido 2,3 p.p. respecto al anterior semestre.

Respecto a la compartición de datos con terceros, el 65,7% de los usuarios declara no compartir todos los archivos que tienen en su ordenador.

Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de infectar el equipo informático de usuarios poco precavidos.



BASE: Usuarios de redes P2P

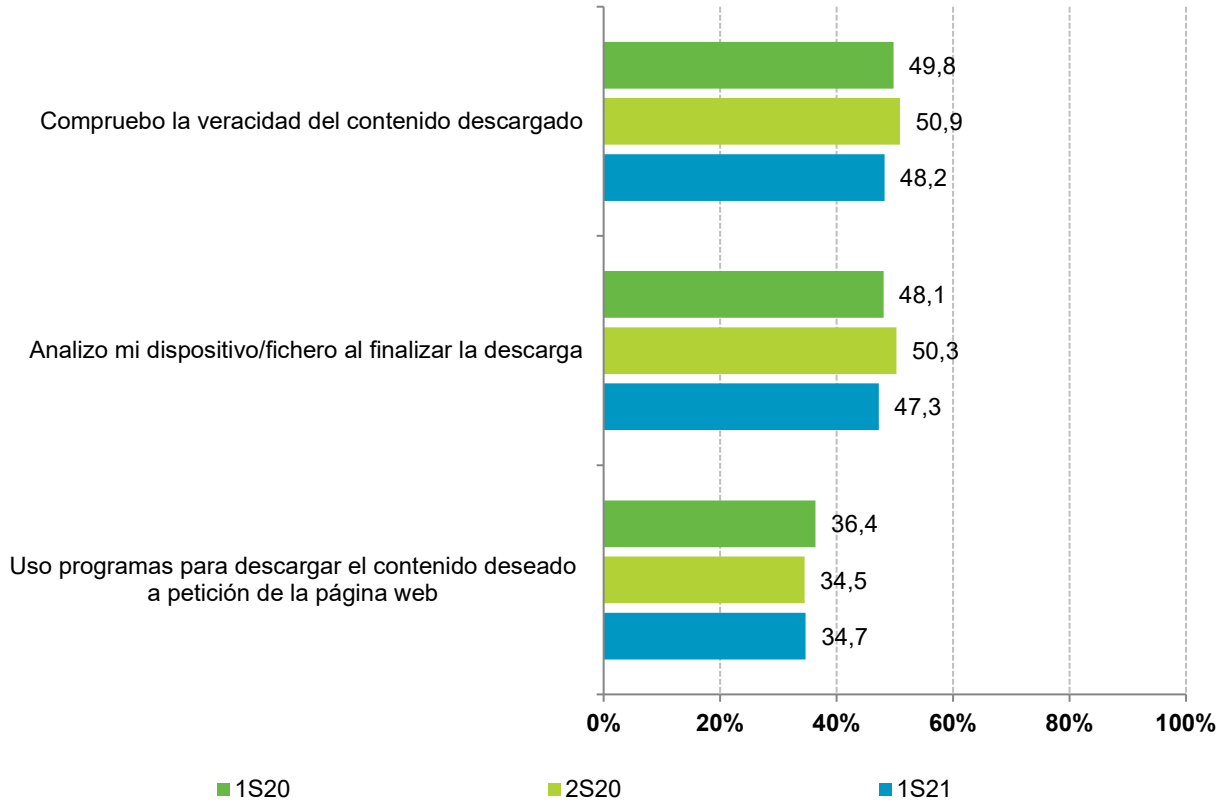
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de descarga directa de archivos, programas, documentos, etc.

Se aprecia un descenso en el uso de herramientas utilizadas por los usuarios para analizar los ficheros que se descargan, aunque también desciende levemente el porcentaje de usuarios que afirmar no comprobar la veracidad del contenido descargado.

Herramientas gratuitas que te ayudarán a proteger tus dispositivos (ordenador, smartphone, tablet) para que tu navegación por Internet, sea lo más segura posible. Disponibles en:

https://www.osi.es/es/herramientas



BASE: Total usuarios

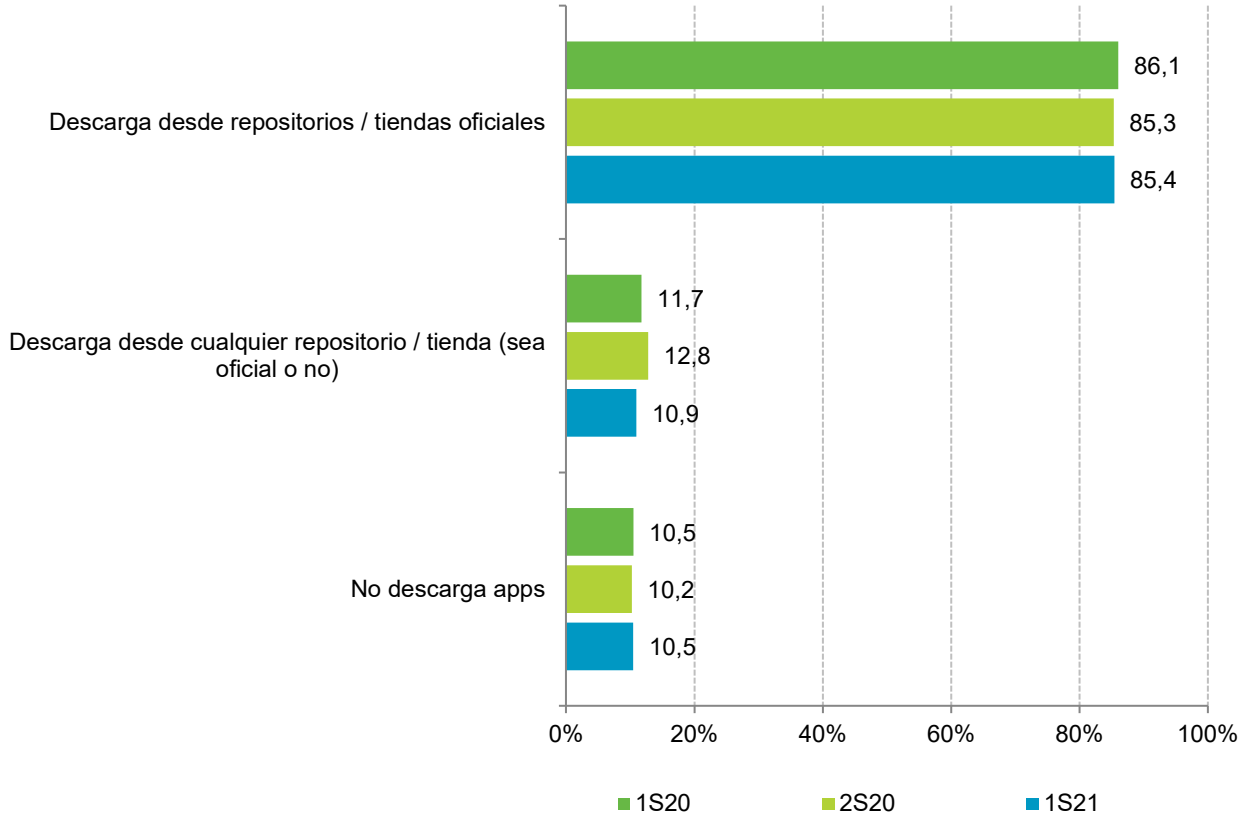
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en la descarga de apps en el smartphone o *tablet*

El 85,4% de los usuarios con dispositivos móviles declaran descargar las apps desde repositorios o tiendas oficiales, porcentaje similar al semestre anterior.

El porcentaje de usuarios que no descargan aplicaciones en sus terminales vuelve a situarse en el 10,5%, mismo dato que hace un año.

¡Ayuda! Instalé una app no fiable
https://www.osi.es/es/campanas/dispositivos-moviles/instale-app-no-fiable



BASE: Usuarios que disponen de dispositivo Android

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

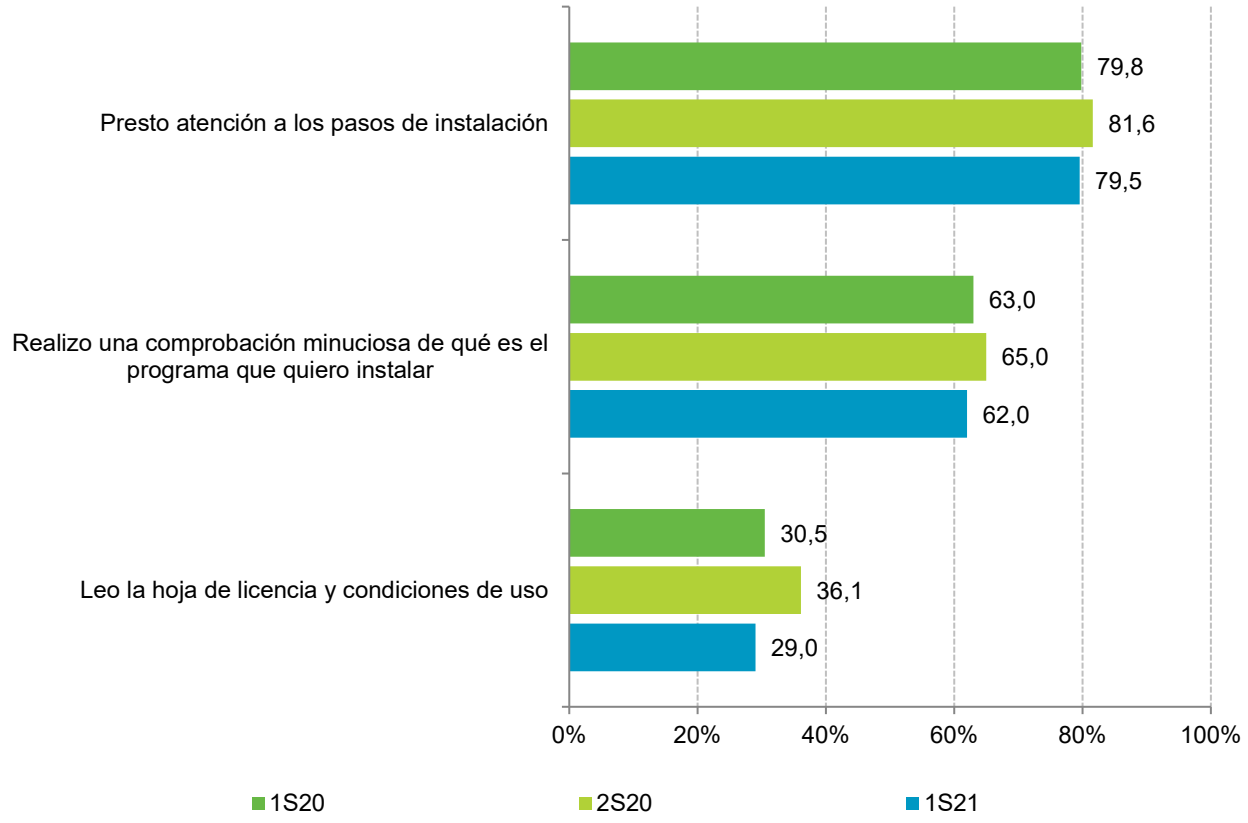
Hábitos de comportamiento en la instalación de programas

Es elevado el porcentaje de usuarios que declaran prestar atención a los pasos cuando instalan un programa en su PC, un 79,5, sin embargo, este dato sufre un descenso de -2,1 p.p. respecto al semestre anterior.

El 29% de los usuarios manifiestan que leen la hoja de licencia y condiciones de uso cuando instalan un *software* en su ordenador, aunque este dato, también desciende durante el primer trimestre del año 7,1 puntos, respecto al último semestre del año 2020.

¿Conoces los peligros de usar páginas de descarga directa?

https://www.osi.es/es/actualidad/blog/2015/02/09/usa-paginas-de-descarga-directa-sin-renunciar-tu-seguridad



BASE: Usuarios de PC

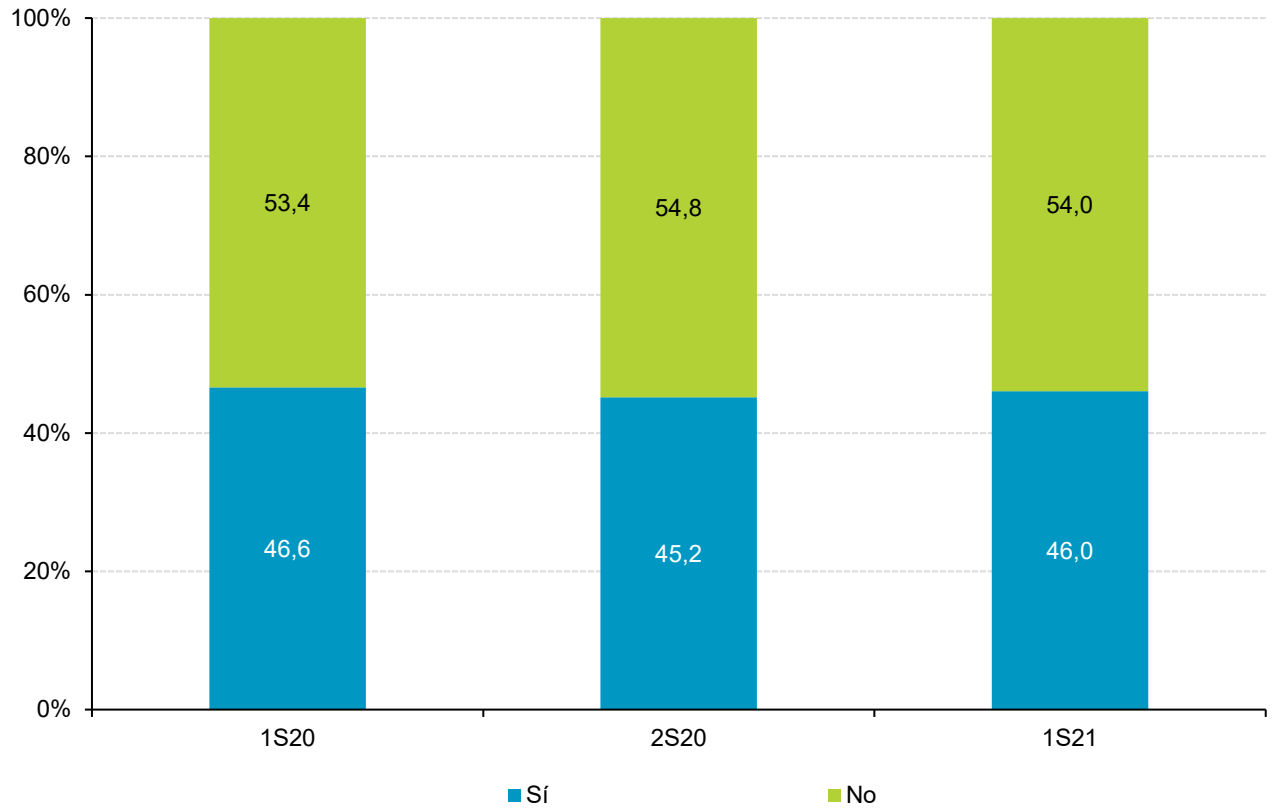
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Lectura y aceptación de la información legal al registrarse o darse de alta en proveedores de servicios en Internet (redes sociales, comercio electrónico, etc.)

Aumenta levemente en 0,8 puntos porcentuales el número de usuarios que declaran leer la información legal antes de registrarse o darse de alta en proveedores de servicios de Internet.

En los últimos meses se ha ofrecido mucha información sobre los cambios en las políticas de privacidad en redes sociales, para la adaptación a los cambios sugeridos por la normativa europea de protección de datos, la GDPR.

Gestión de riesgo y evaluación de impacto en tratamientos de datos personales
https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd



BASE: Total usuarios

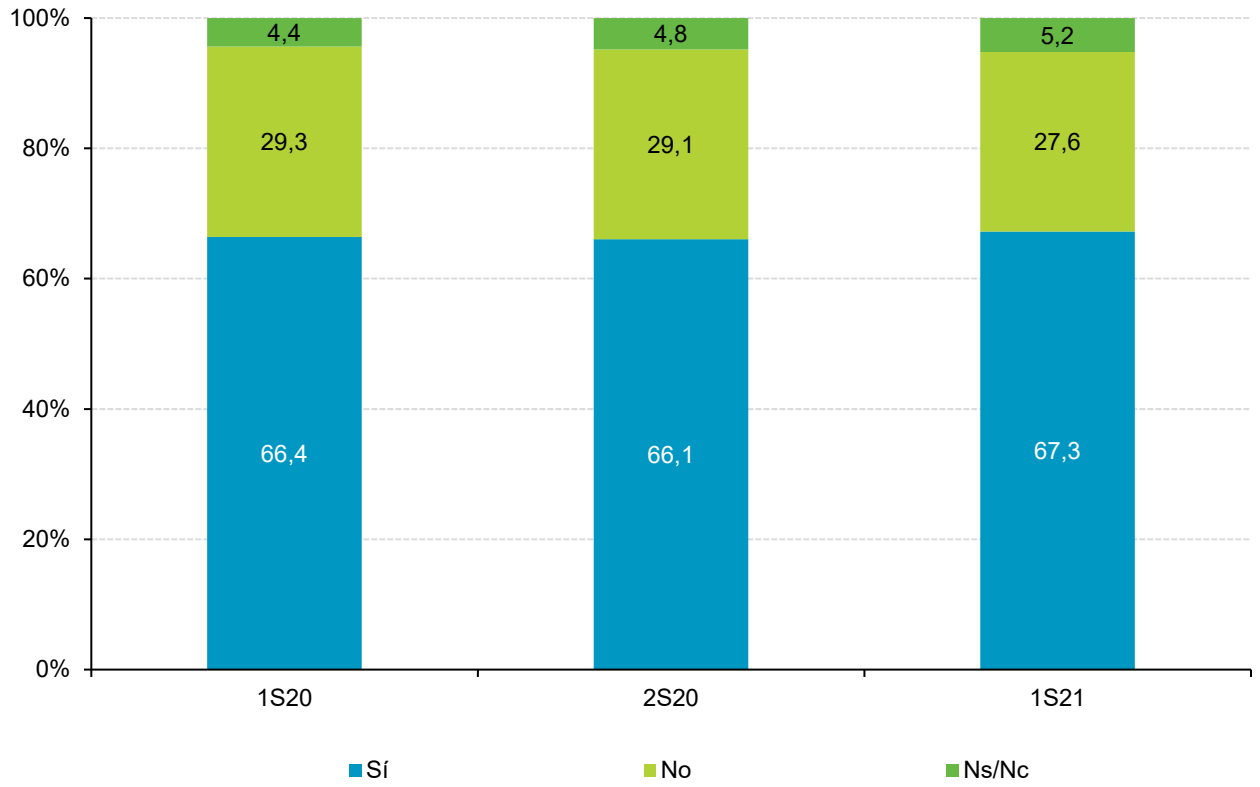
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Comprobación de permisos al instalar apps

Al instalar aplicaciones, se solicita tener permiso a ciertos recursos del teléfono y al conceder dichos permisos, se está permitiendo tener acceso a dichos recursos, por lo que es importante comprobar que se está autorizando.

En este sentido, durante el primer semestre del año, aumenta el porcentaje de usuarios que comprueban los permisos al instalar aplicaciones (+1,2 p.p.), en concreto, el 67,3%.

Permisos de apps y riesgos para tu privacidad
https://www.osi.es/es/permisos-de-apps-y-riesgos-para-tu-privacidad



BASE: Usuarios que disponen de dispositivo Android y descargan apps

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

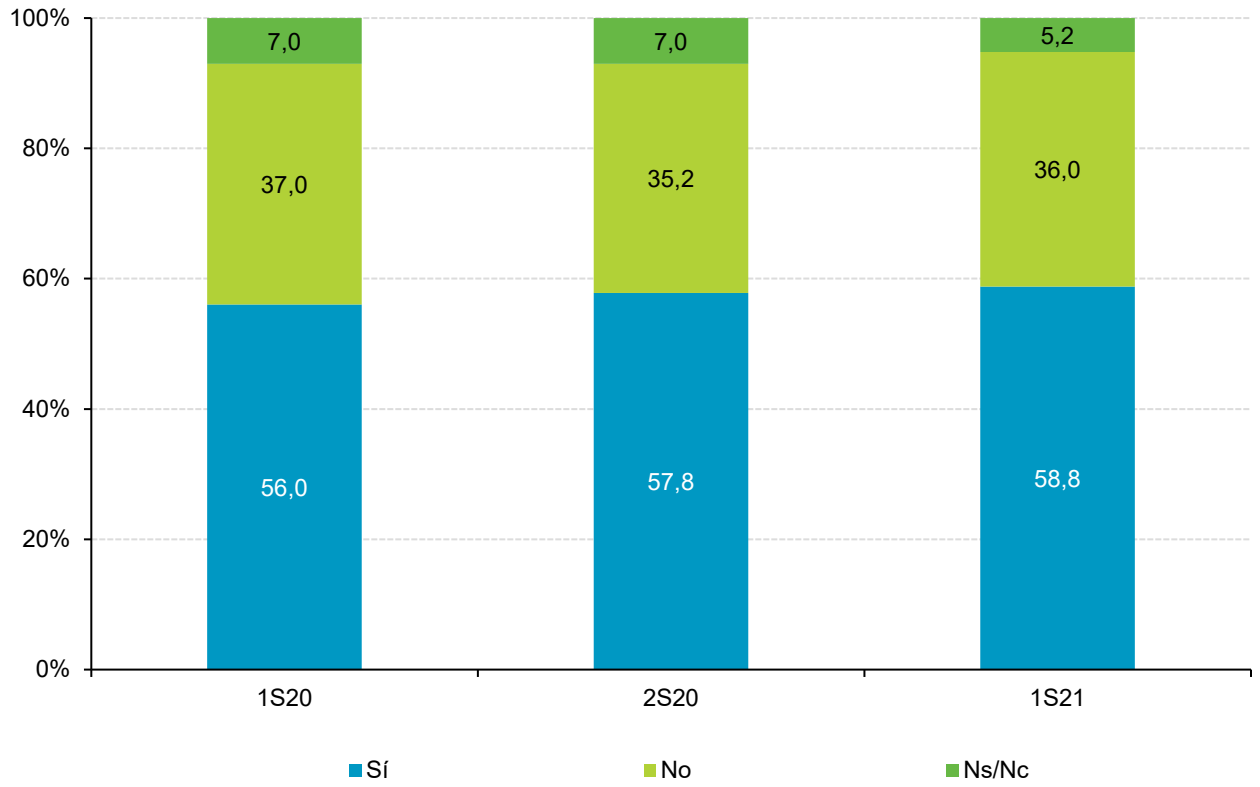
Verificación del origen al instalar apps

Continua en aumento leve pero constante, el número de usuarios que declaran verificar el origen de las aplicaciones antes de instalarlas, en concreto, un punto porcentual más que en el semestre anterior y 2,8 puntos respecto a un año antes.

¿Te has parado a pensar en los permisos que estás dando a la apps que instalas?

https://www.osi.es/es/campanas/dispositivos-moviles/acepto-no-acepto

https://www.osi.es/es/actualidad/historias-reales/2019/04/17/por-que-piden-tantos-permisos-las-apps



BASE: Usuarios que disponen de dispositivo Android y descargan apps

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Privilegios del usuario en el dispositivo Android

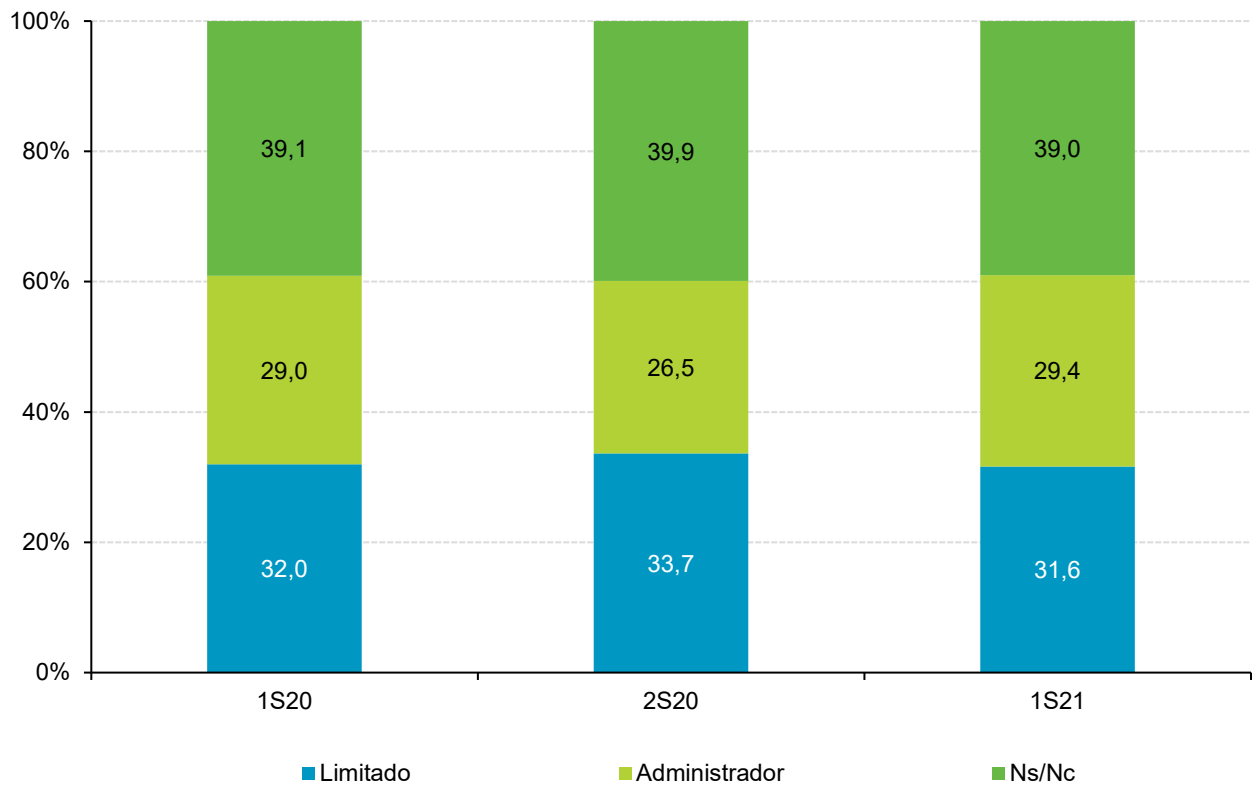
Crece 2,9 puntos porcentuales respecto del semestre anterior, el porcentaje de usuarios que declaran que sus dispositivos operan en modo administrador y se sitúa en el 29,4% de los casos.

Por otro lado, el 39% de usuarios desconoce si su dispositivo Android opera con privilegios de administrador o no.

Se conoce como "rooteo" o "rootear" a la obtención de privilegios de administrador (root). Esto permite al usuario acceder y modificar cualquier aspecto del sistema operativo. Pero también existen riesgos ya que el malware puede aprovecharse de esto logrando un mayor control y/o acceso al dispositivo.

Más información:

https://www.osi.es/es/actualidad/blog/2019/04/24/conocias-el-termino-jailbreaking-o-rooting



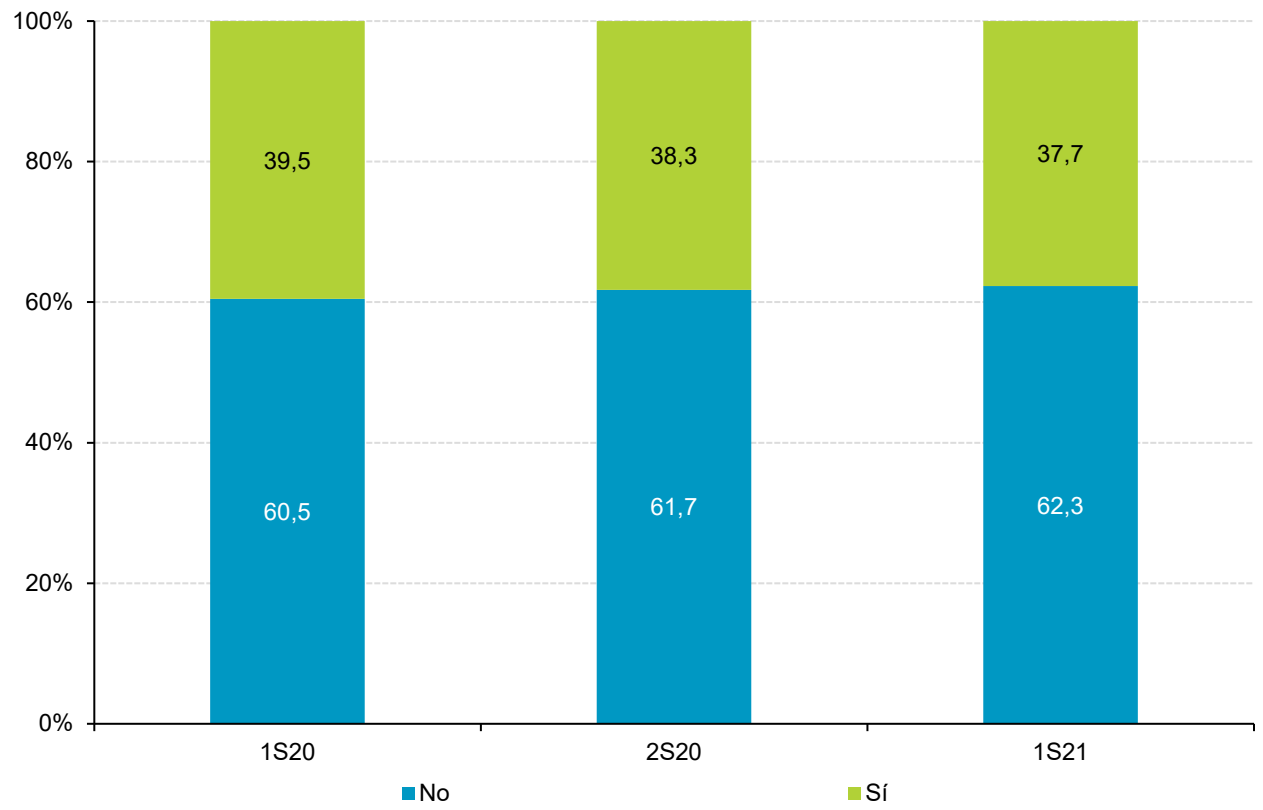
BASE: Usuarios que disponen de dispositivo Android

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Realización consciente de alguna conducta de riesgo

La evolución de las conducta de riesgo continua experimentando una leve mejoría respecto a semestres anteriores.

En concreto, el 62,3% de los usuarios declaran no realizar conductas de riesgo de forma consciente, lo que supone una mejora porcentual intersemestral de 0,6 p.p., y de 1,8 puntos interanual.



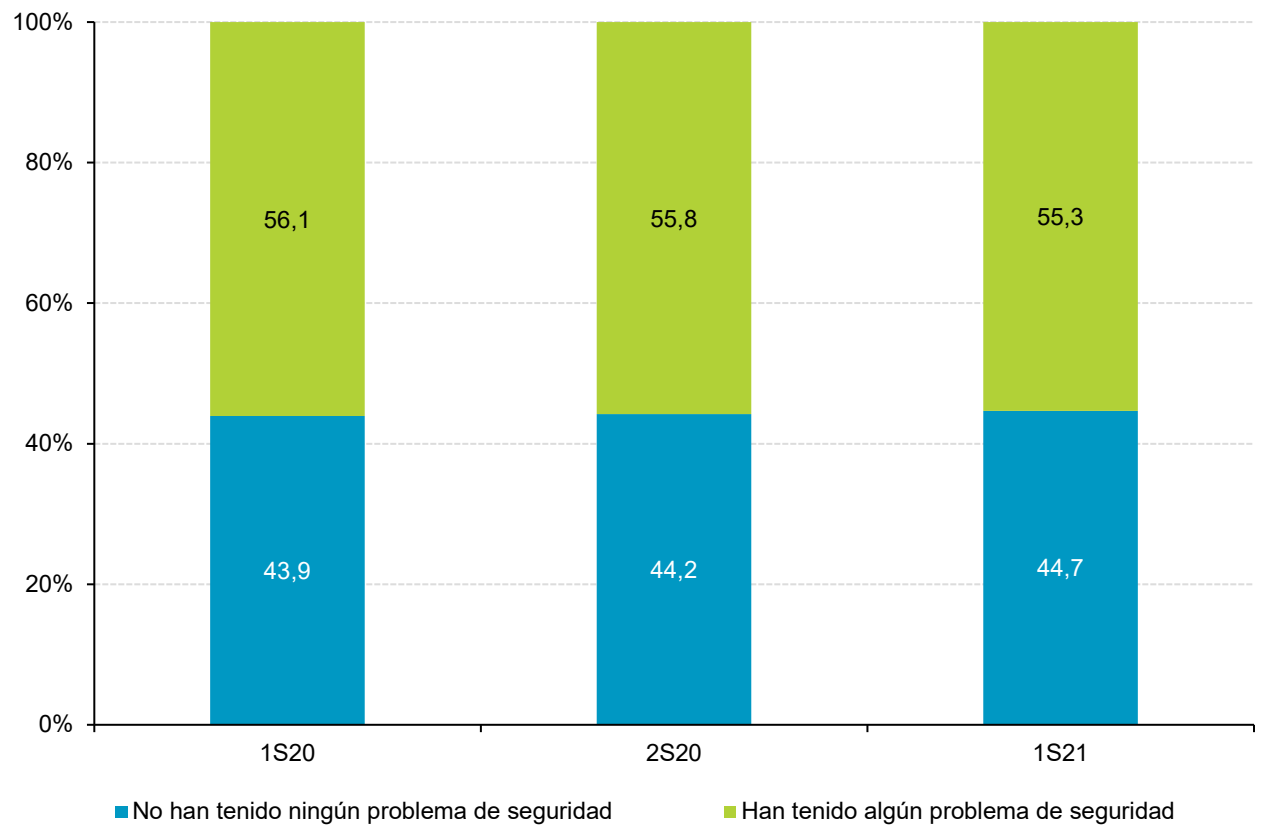
BASE: Total usuarios

Módulo IV:
Incidencias de seguridad

Módulo IV: Incidencias de seguridad

Incidencia de seguridad en los últimos seis meses en el dispositivo con el que se accede habitualmente a Internet

El 55,3% de los panelistas afirma haber sufrido alguna incidencia de ciberseguridad durante el primer semestre de 2021, dato algo inferior al registrado durante el semestre anterior, que fue del 55,8%. Es un pequeño descenso, pero paulatino desde el primer semestre de 2020.



BASE: Total usuarios

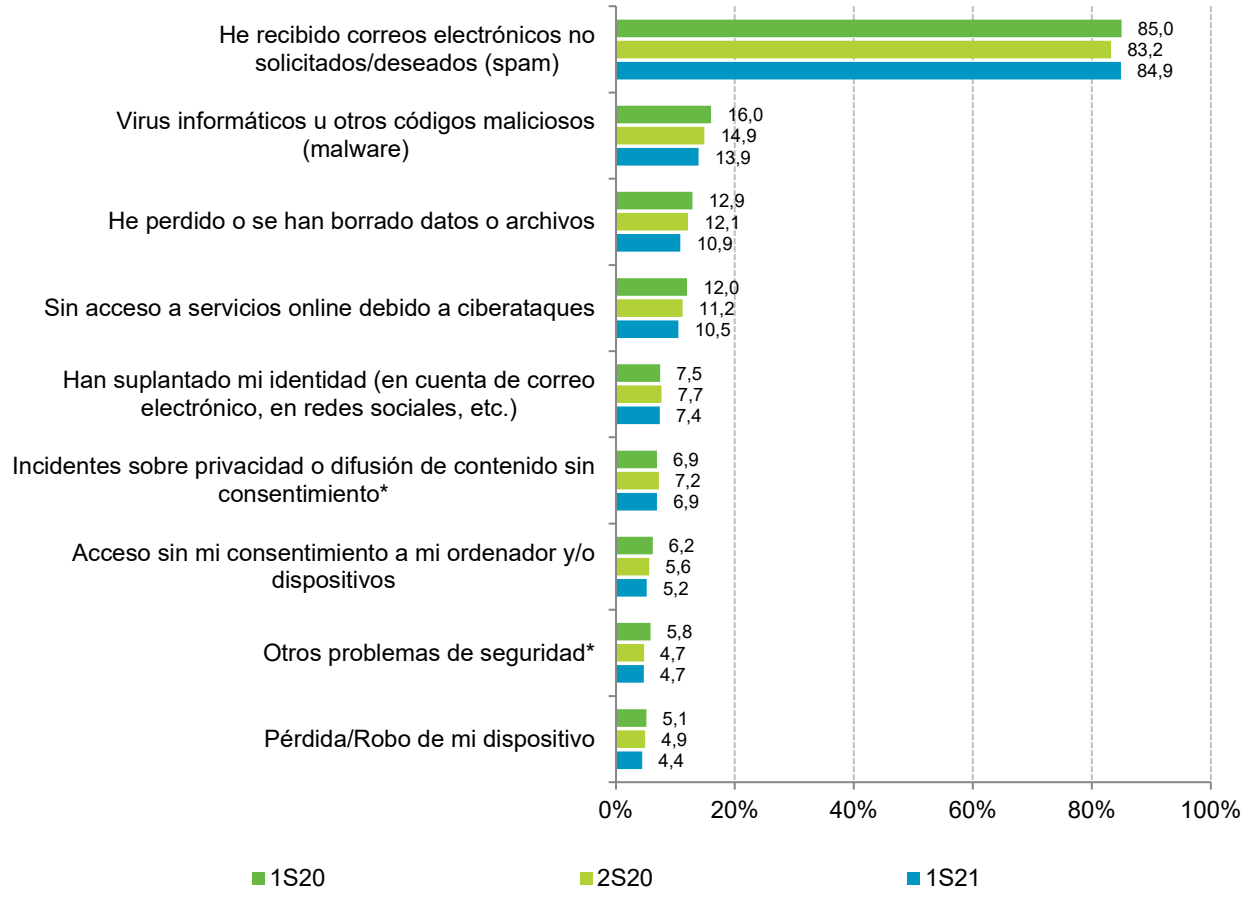
Módulo IV: Incidencias de seguridad

Problemas de seguridad acontecidos en los últimos seis meses en el dispositivo con el que se accede habitualmente a Internet

En cuanto a las incidencias de seguridad padecidas por los panelistas, la recepción de correos indeseados ocupa el primer lugar con un 84,9% de los casos. Es un dato algo mayor que el registrado en el primer semestre del año. En segundo lugar están los virus informáticos, aunque en este caso según los datos recogidos, disminuye en 1 p.p. respecto al semestre anterior.

La suplantación de identidad puede conducir a otros ciberataques. Protégete y reacciona ante la suplantación de identidad
https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

Guía OSI sobre ciberataques:
https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf



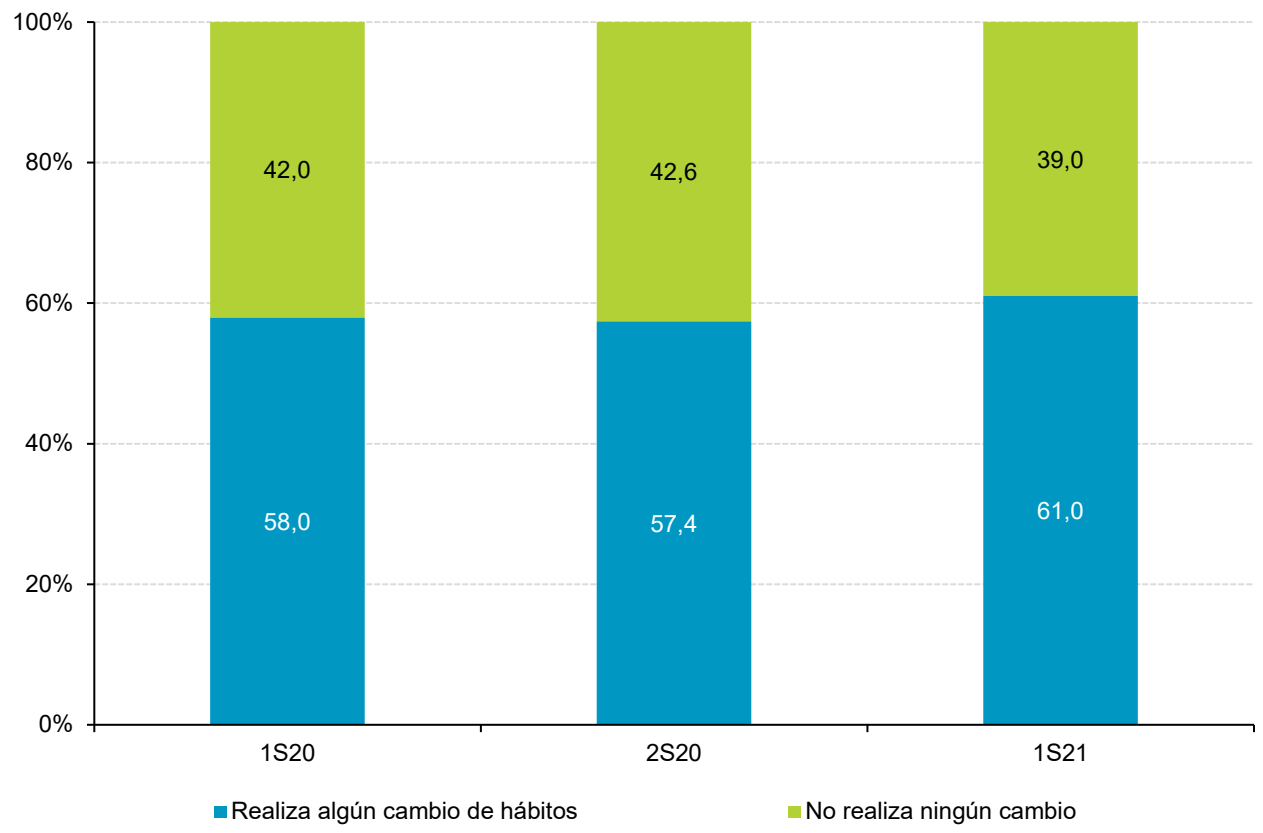
*nuevas categorías

BASE: Usuarios que han sufrido alguna incidencia de seguridad

Módulo IV: Incidencias de seguridad

Realización de cambio de hábitos en Internet motivados por las incidencias de seguridad experimentadas durante los últimos seis meses

En el 61% de los casos, los usuarios que han experimentado algún incidente de seguridad, han realizado algún cambio en sus hábitos a la hora de navegar por Internet tras haber sufrido la incidencia. La diferencia respecto del semestre anterior es de +3,6 p.p.



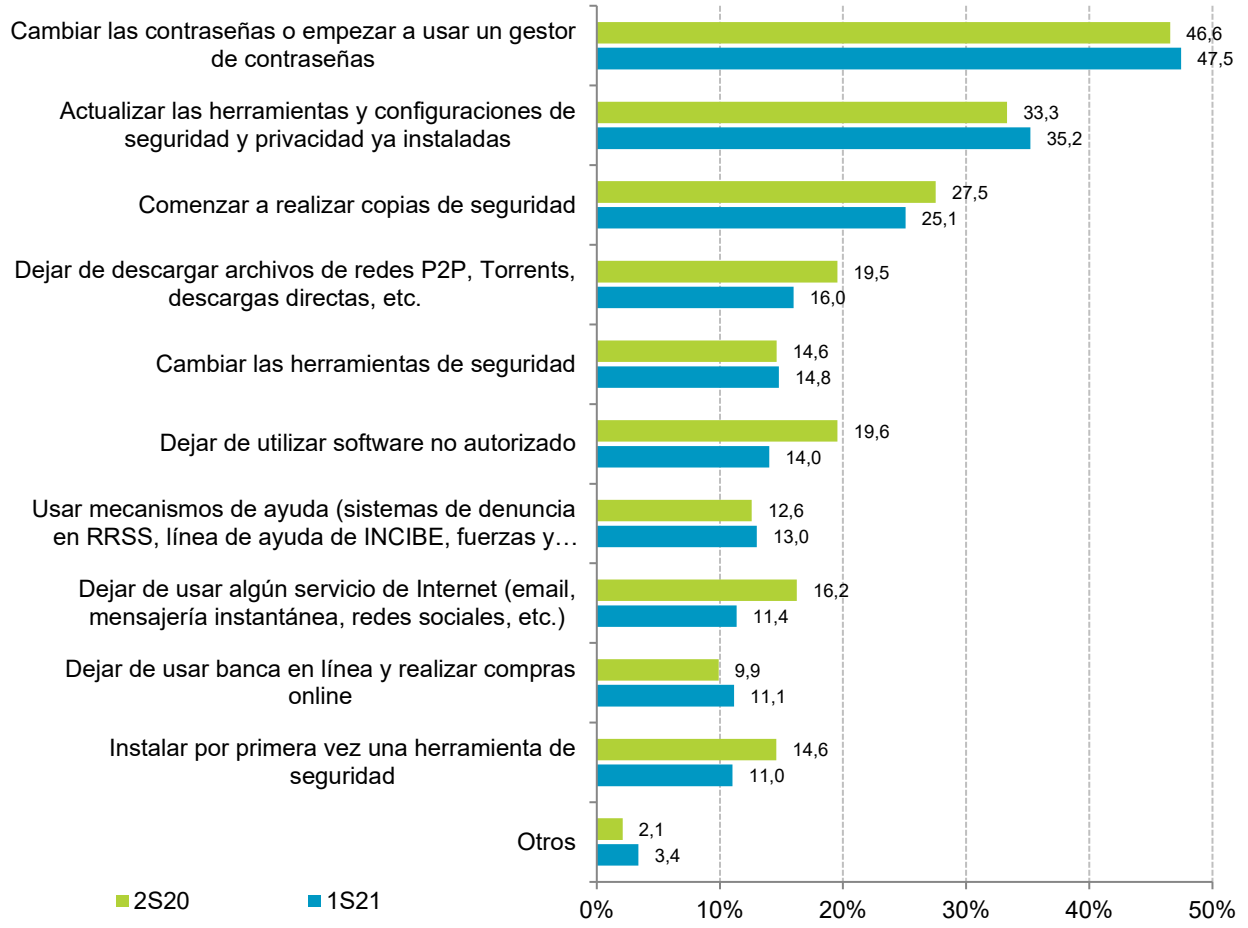
BASE: Usuarios que han sufrido alguna incidencia de seguridad

Módulo IV: Incidencias de seguridad

Cambios de hábitos en Internet motivados por las incidencias de seguridad experimentadas durante los últimos seis meses

Los cambios más habituales realizados tras sufrir un problema de seguridad, son el cambio de contraseña o empezar a utilizar un gestor de contraseñas y la actualización de herramientas de privacidad, con 47,5% (+0,9 p.p.) y 35,2% (+1,9 p.p.), respectivamente.

Asimismo, es reseñable el hecho de que tras experimentar un problema de seguridad, el 14% de los usuarios ha dejado de usar *software* no autorizado y el 11,4% han dejado de usar algún servicio de Internet como el mail, mensajería instantánea o redes sociales, lo que supone un descenso intersemestral de -5,6 p.p. y 4,8 p.p., respectivamente.

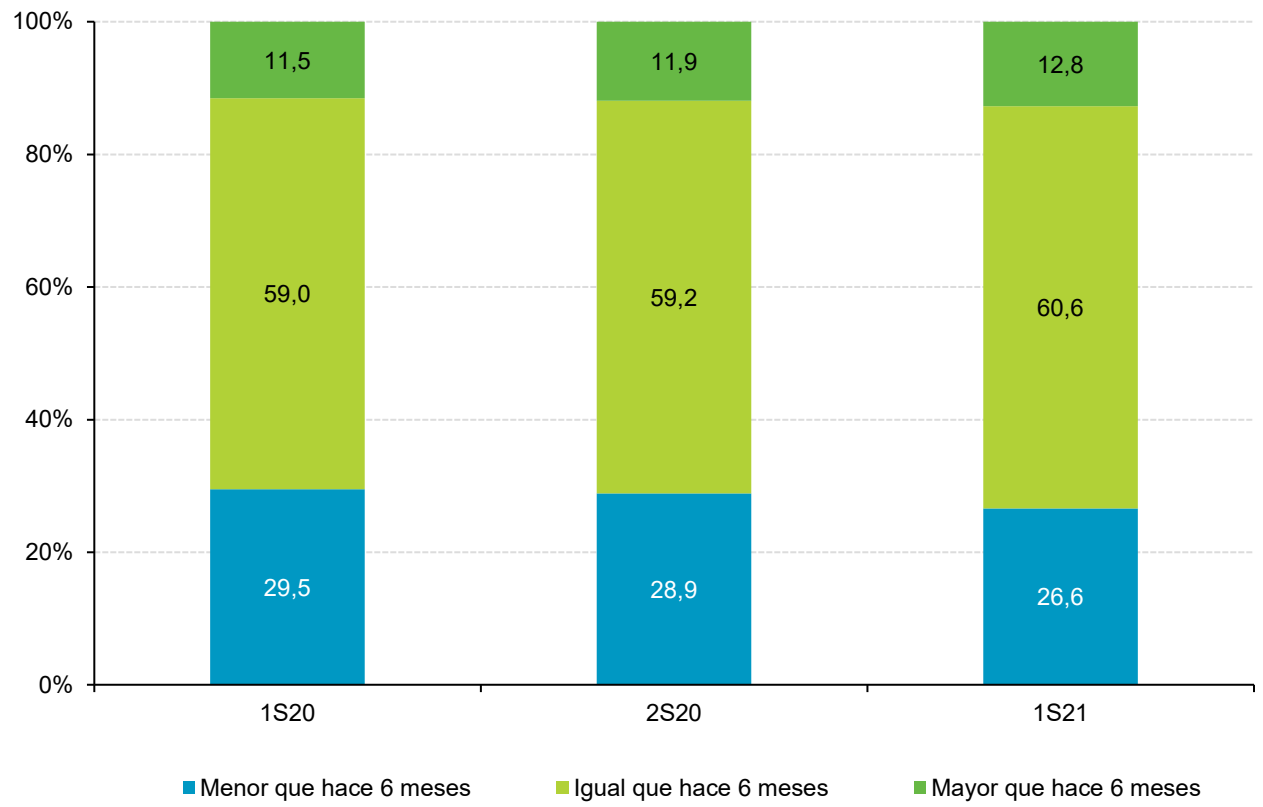


BASE: Usuarios que han sufrido alguna incidencia de seguridad y modifica sus hábitos

Módulo IV: Incidencias de seguridad

Percepción del usuario respecto al número de incidentes de seguridad que ha sufrido

La percepción de los usuarios respecto al número de problemas de seguridad experimentados durante el primer semestre de 2021, es ligeramente superior a la que tenían durante el último semestre de 2020, concretamente el valor se sitúa en el 12,8% de los usuarios, lo que supone un leve incremento de 0,9 p.p. intersemestral

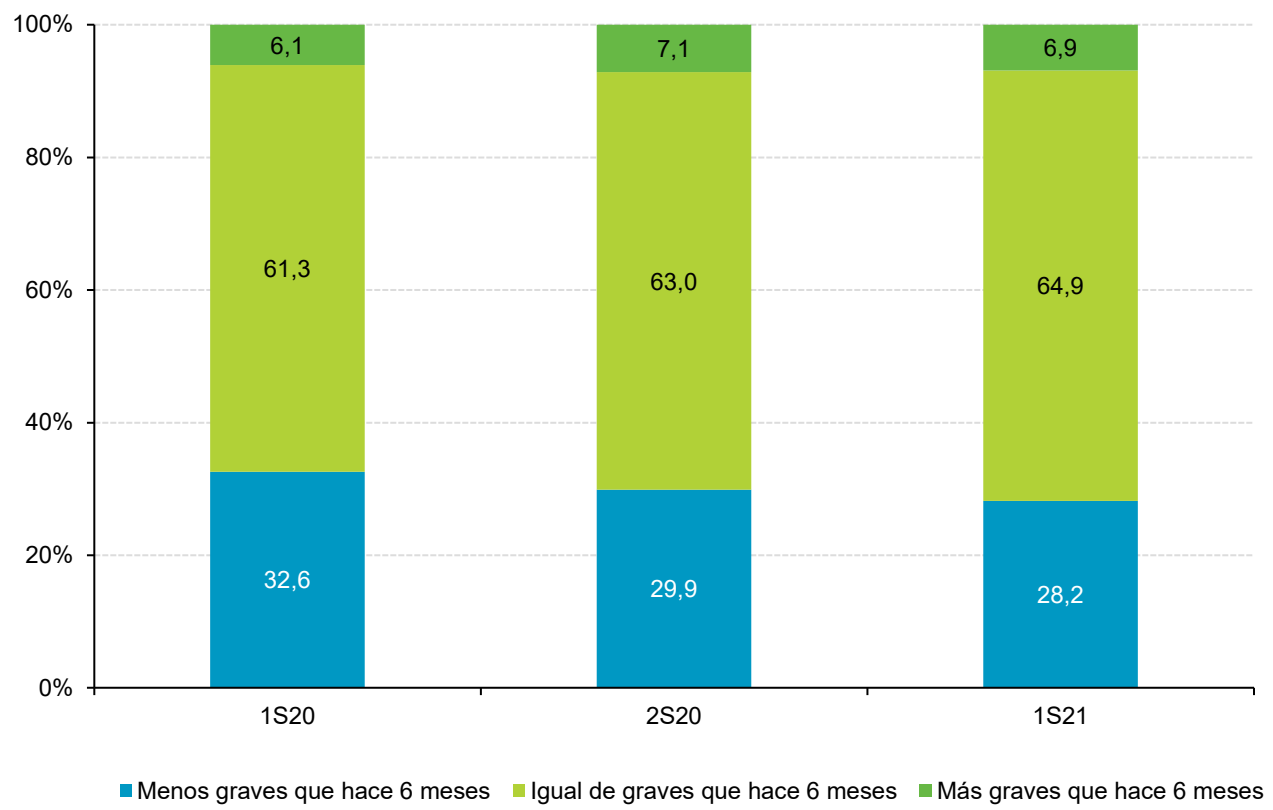


BASE: Total usuarios

Módulo IV: Incidencias de seguridad

Percepción del usuario al respecto a la gravedad de los incidentes de seguridad que ha sufrido

En cuanto a la gravedad de los incidentes sufridos, el 64,9% de los usuarios perciben que la gravedad de las incidencias se ha mantenido prácticamente igual respecto al semestre anterior, mientras que desciende levemente los usuarios que declaran haber sufrido incidentes más graves (-1,7 p.p.)



BASE: Total usuarios

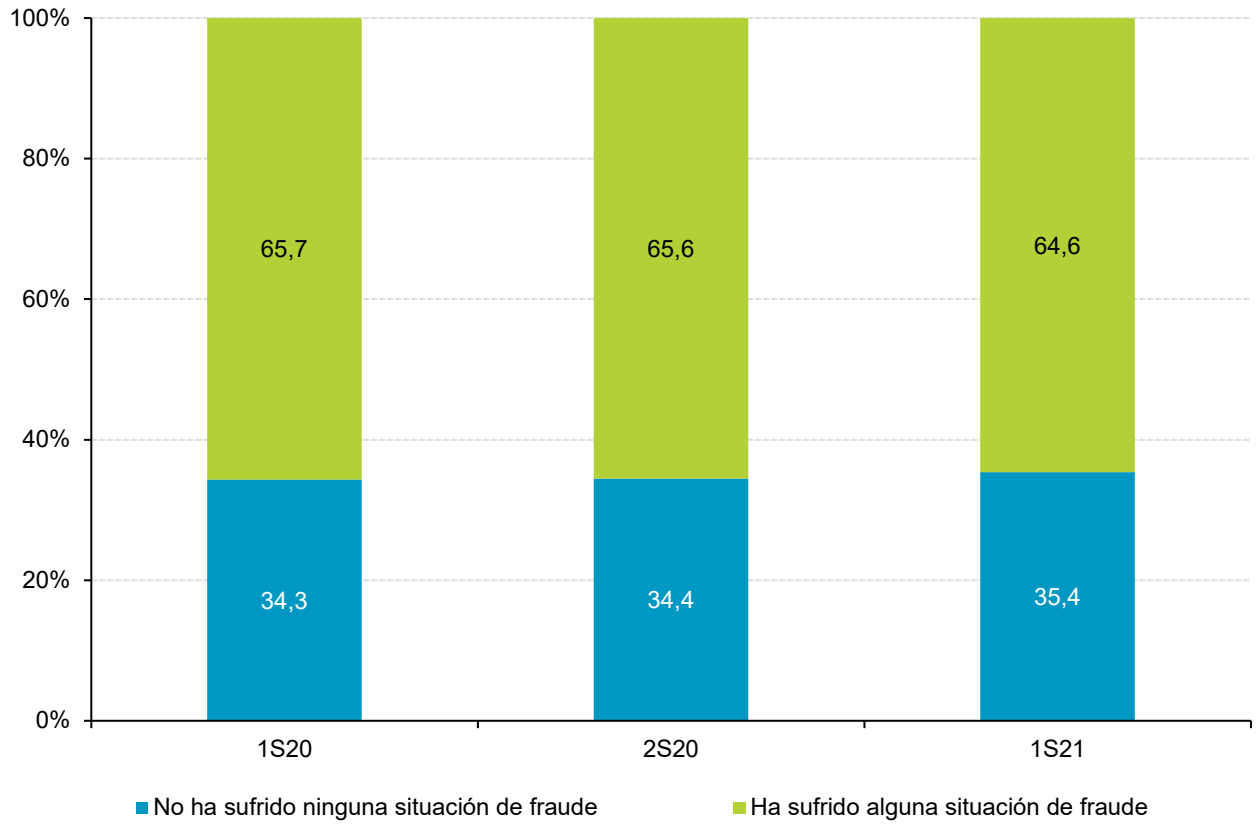
Módulo V:
Fraude

Módulo V: Fraude

Ocurrencia de alguna situación de fraude en los últimos seis meses

A diferencia de otras incidencias de seguridad que pueden ser más subjetivas desde el punto de vista del usuario, como las infecciones por *malware*, en el caso del fraude, al afectar al plano económico, las víctimas de este incidente son más conscientes de la situación.

En este sentido, el 64,6% de los panelistas han declarado haber sufrido alguna situación de fraude durante el semestre, lo que significa una disminución de 1 p.p. respecto al semestre anterior.



¿Sabes como denunciar el fraude online?
https://www.osi.es/es/reporte-de-fraude

BASE: Total usuarios

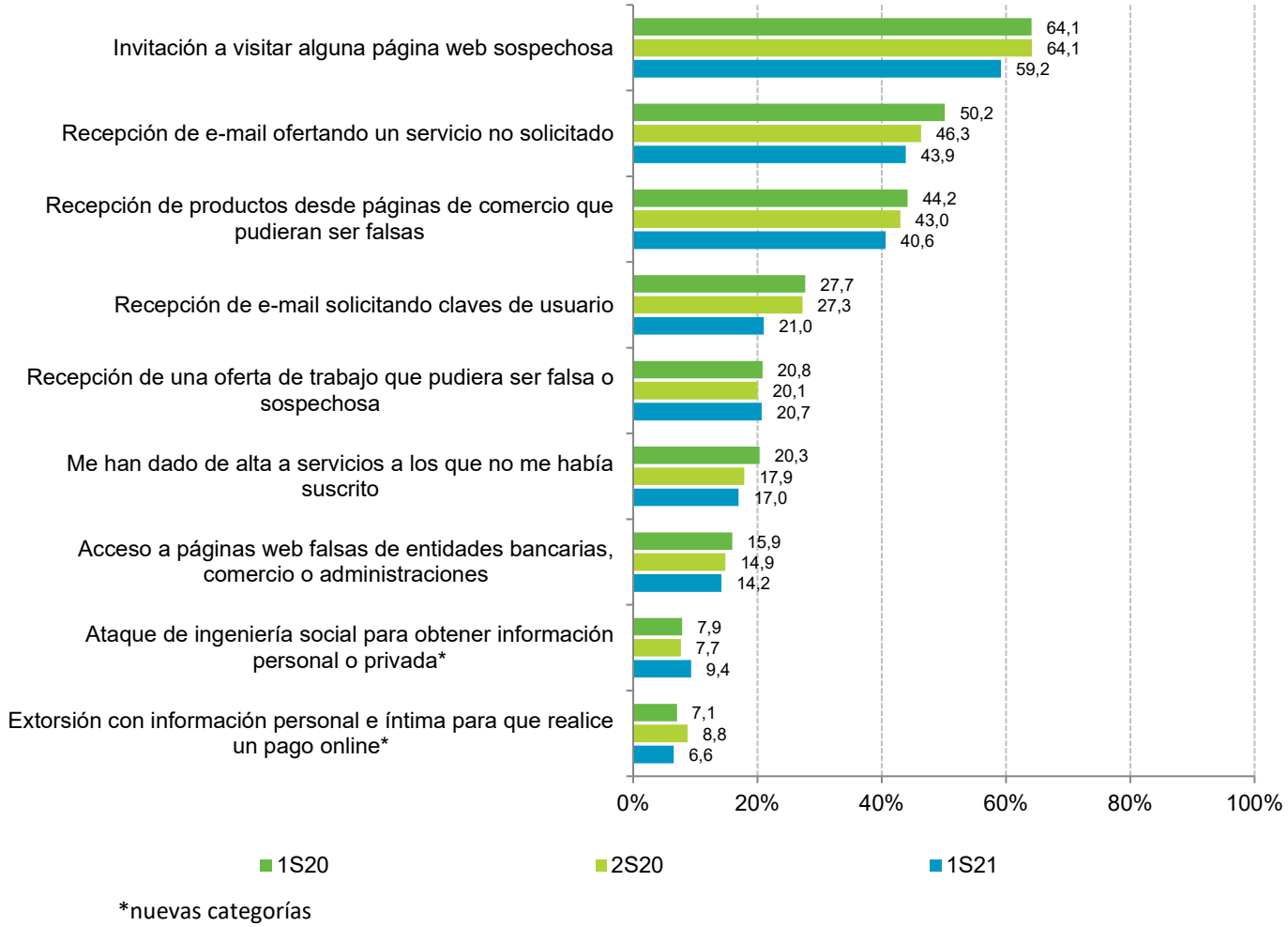
Módulo: Fraude

Situaciones de fraude ocurridas en los últimos seis meses

El intento de fraude más destacado por los panelistas sigue siendo la invitación a visitar webs sospechosas 59,2%, no obstante, disminuye 4,9 p.p. respecto del semestre anterior.

Aunque en general se observa que han disminuido los intentos de estafa, en este semestre, los ataques de ingeniería social, que implican manipulación para obtener información confidencial, han aumentado en 1,7 p.p.

¿Sabes como identificar el fraude online?
https://www.osi.es/es/guia-fraudes-online



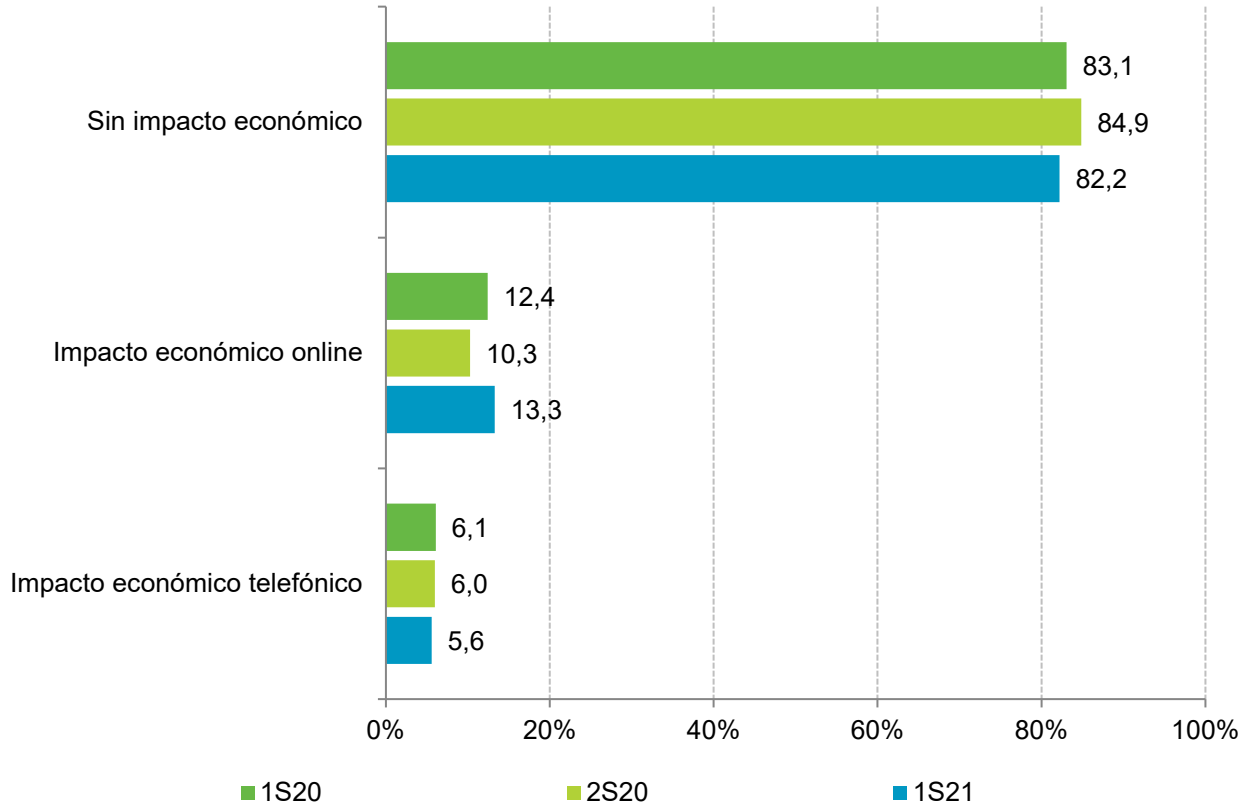
*nuevas categorías

BASE: Usuarios que han sufrido alguna situación de fraude

Módulo V: Fraude

Perjuicio económico debido a posibles fraudes

Sobre el impacto económico y durante el primer semestre de 2021, el 13,3% de los usuarios que han sufrido una situación de fraude, declaran haber experimentado un impacto económico a través de Internet, lo que se traduce en un aumento en 3 p.p. sobre el semestre anterior.



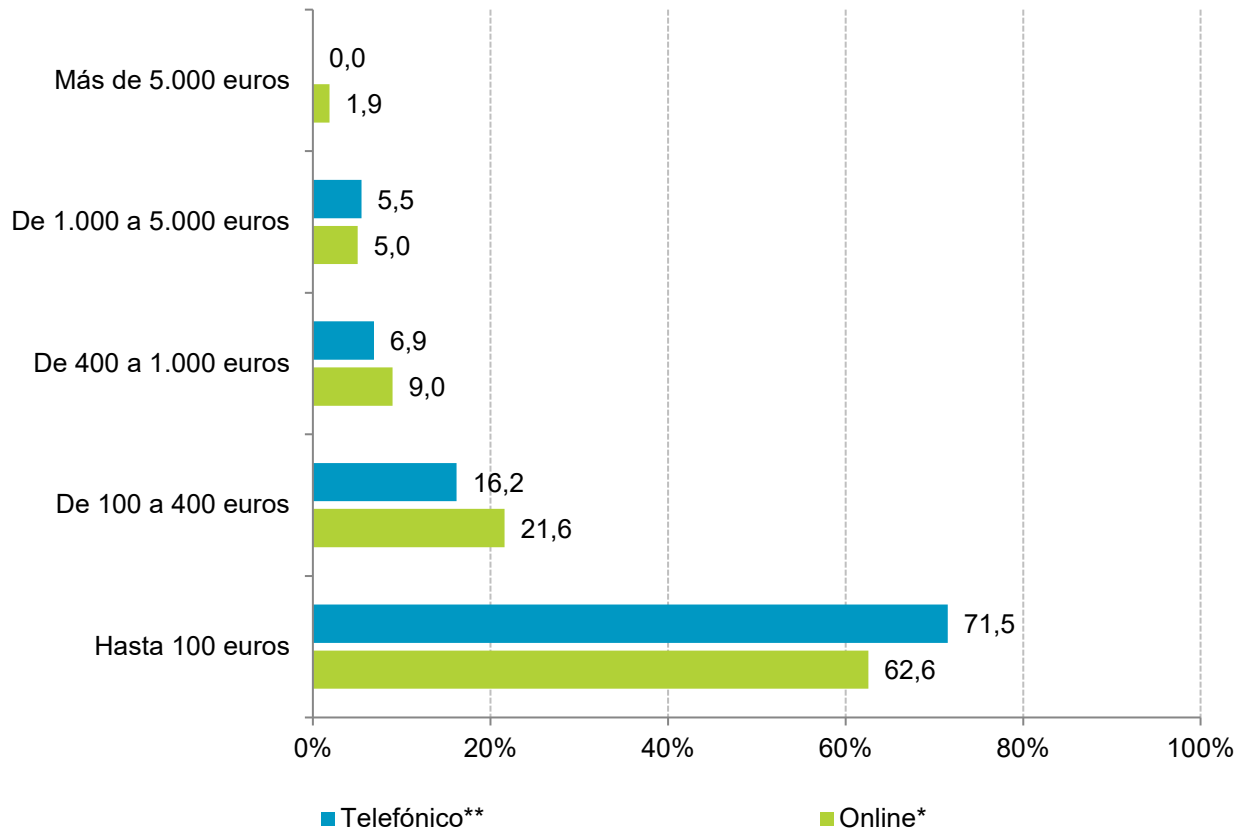
BASE: Usuarios que han sufrido alguna situación de fraude

Módulo V: Fraude

Distribución del perjuicio económico debido a posibles fraudes

El 71,5% de los usuarios que han sido afectados por algún fraude, mantiene que ha tenido perdidas inferiores a 100 euros por medio de un fraude telefónico o vishing, frente al 62,6% que declaran haber sido estafados online con la misma cantidad.

Para cantidades que oscilan entre 100 y 400 euros, el fraude online es superior al telefónico, 21,6% vs 16,2%.



*** BASE: Usuarios que han sufrido perjuicio económico debido a un fraude online**
**** BASE: Usuarios que han sufrido perjuicio económico debido a un fraude telefónico**

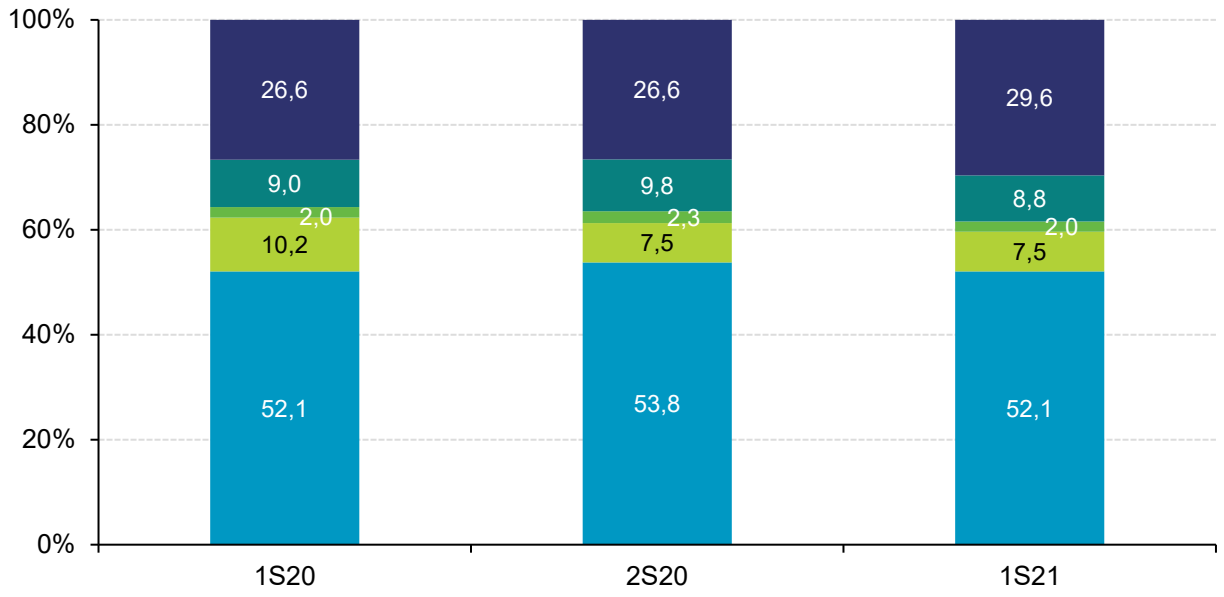
Módulo V: Fraude

Modificación de hábitos en la compra online a causa de la situación de fraude sufrida

Según declaran los usuarios, el 29,6% ha modificado sus hábitos de compra tras sufrir una situación de fraude y ahora realizan comprobaciones básicas según las recomendaciones dadas, porcentaje que aumenta en 3 p.p. respecto al ultimo semestre de 2020.

Pautas básicas para identificar ofertas y webs promocionales a la hora de realizar compras online:

https://www.osi.es/es/campanas/compras-seguras-online



*nueva categoría

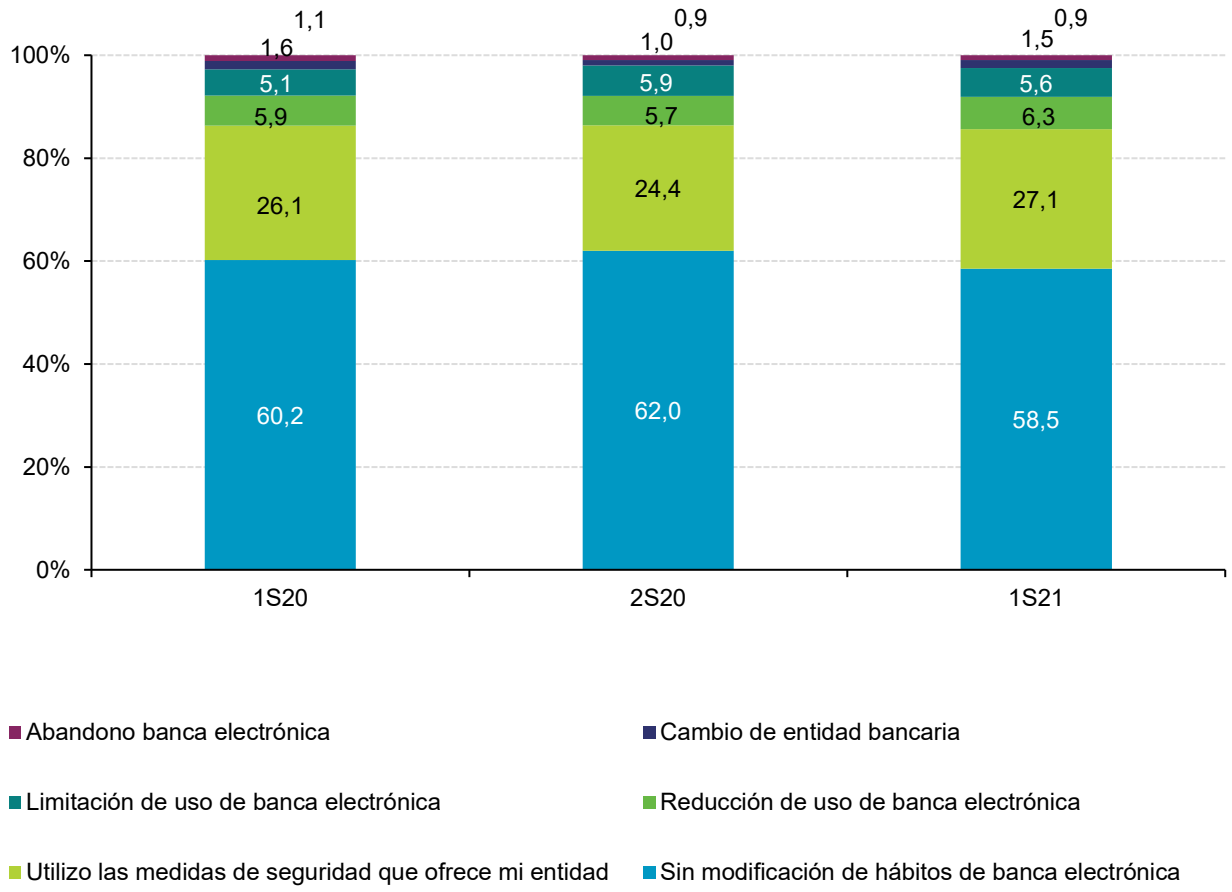
BASE: Usuarios que usan comercio electrónico y han sufrido alguna situación de fraude o perjuicio económico

Módulo V: Fraude

Modificación de hábitos en el uso de banca online a causa de la situación de fraude sufrida

Como ocurre con los hábitos de compra, aumenta respecto a semestres anteriores el número de usuarios que declaran emplear las medidas de seguridad que, en este caso, les ofrece su entidad bancaria (27,1%).

Las entidades bancarias están continuamente implementado controles de seguridad y obligan a sus usuarios a usarlos.



BASE: Usuarios que usan banca online y han sufrido alguna situación de fraude o perjuicio económico

Módulo VI:
Seguridad en Wi-Fi

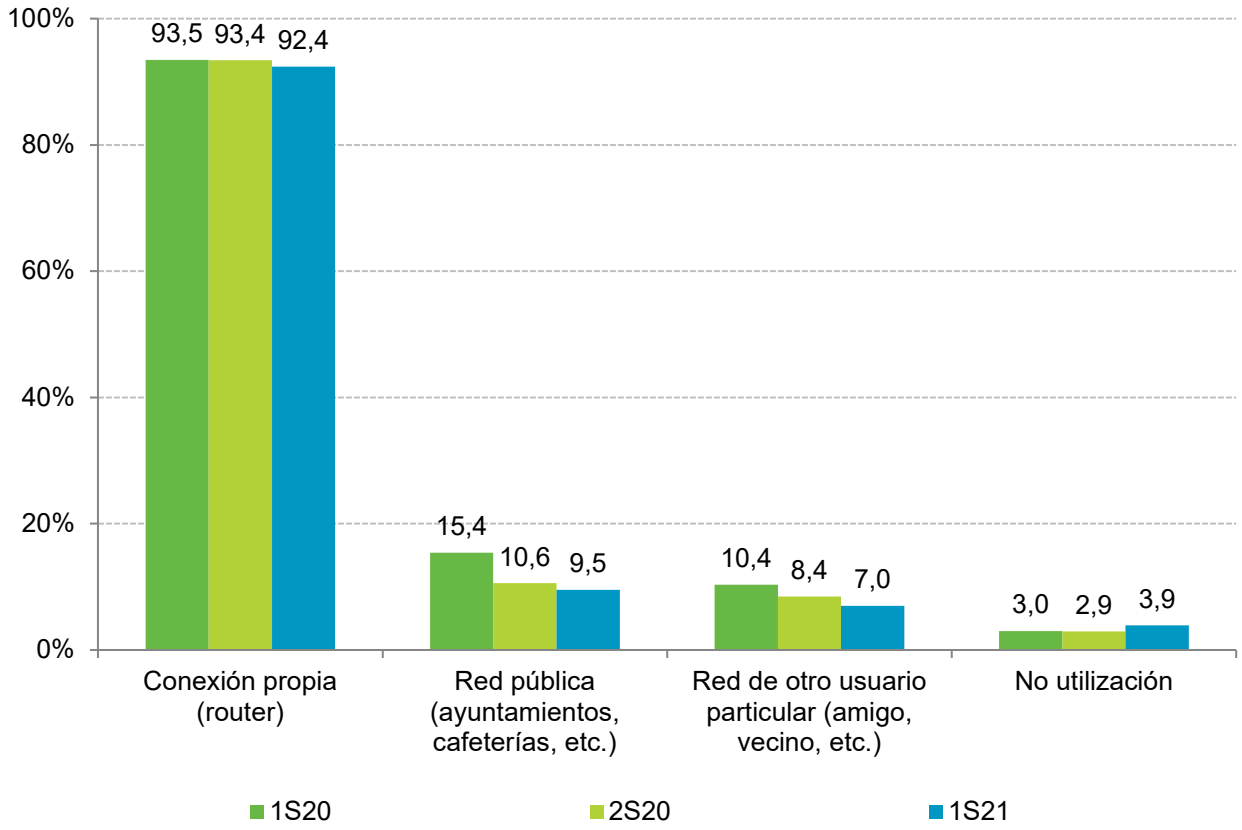
Módulo VI: Seguridad en Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Continúa en descenso el uso de redes públicas o de otros usuarios para conectarse a Internet, según manifiestan los usuarios.

Comparando las declaraciones de este semestre con las del semestre anterior, se observa que el acceso a redes públicas, casi siempre abiertas, ha descendido 1,1 puntos. Es una buena noticia, ya que los usuarios comienzan a concienciarse sobre los peligros que entraña el uso de redes abiertas.

Protección y seguridad al navegar por Internet. Conexiones seguras. https://www.osi.es/es/conexiones-seguras



BASE: Total usuarios

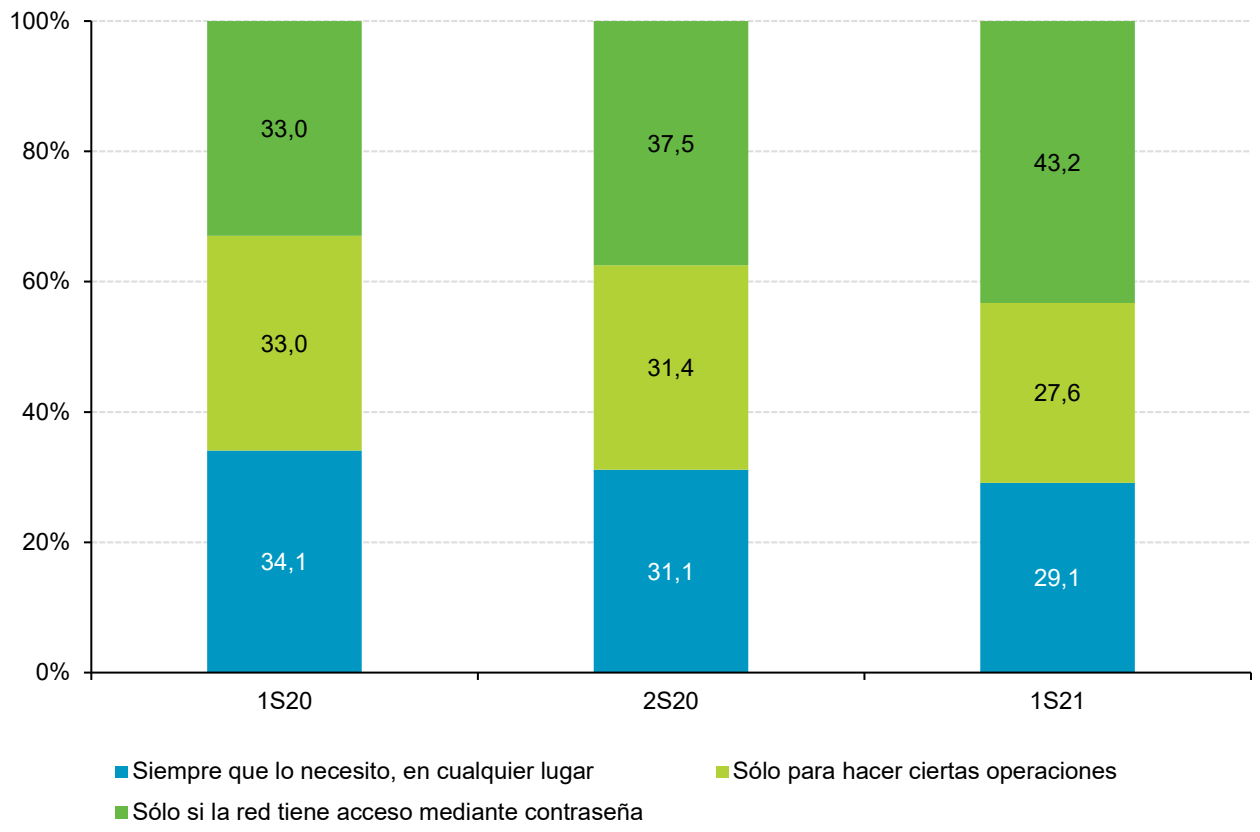
Módulo VI: Seguridad en Wi-Fi

Motivo de uso de redes inalámbricas Wi-Fi públicas o de terceros

Por tercer semestre consecutivo, gran parte de los usuarios declaran usar redes solo si tienen acceso mediante contraseña.

El aumento respecto al semestre anterior es significativo, ya que se cifra en 5,7 p.p.

Cómo conectarte a redes Wi-Fi públicas de forma segura:
https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil



BASE: Usuarios que se conectan a una red Wi-Fi pública o de otro usuario

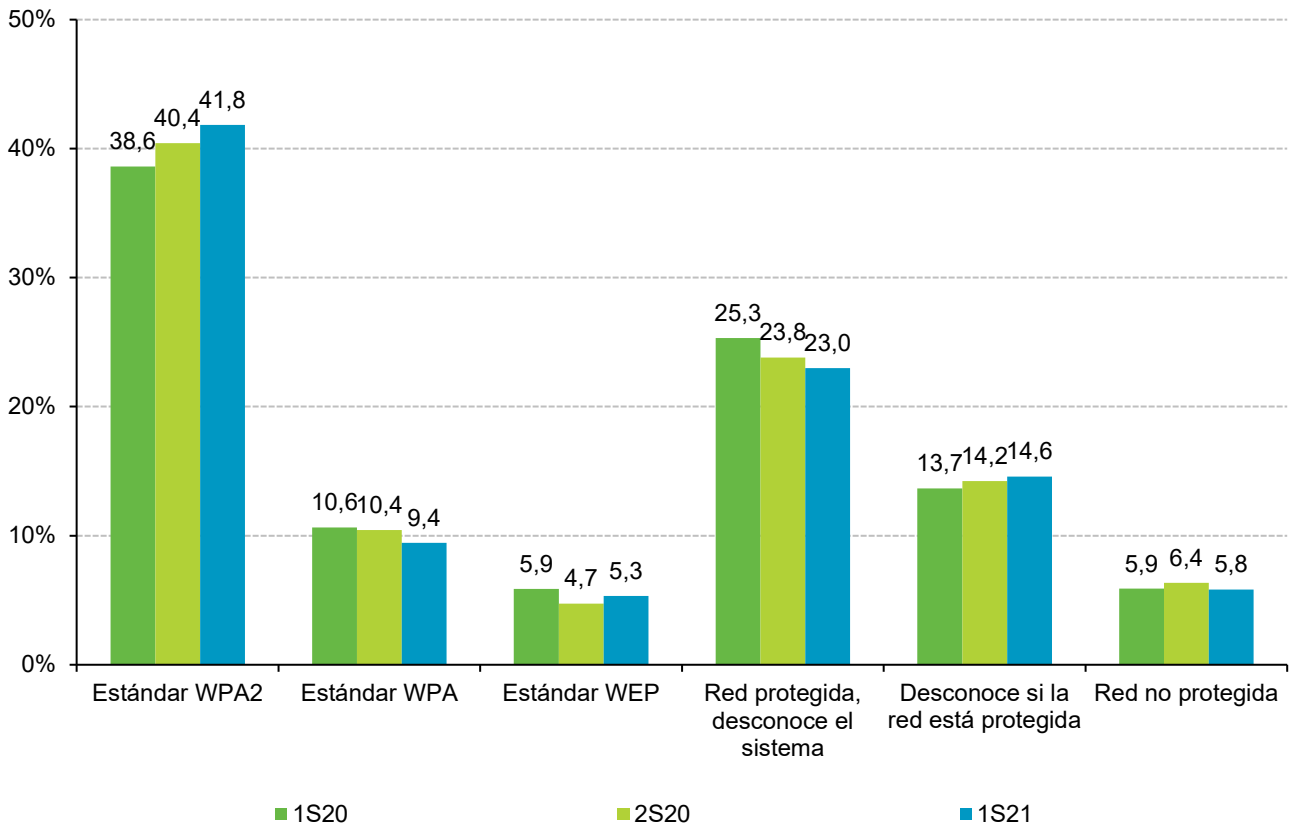
Módulo VI: Seguridad en Wi-Fi

Sistema de seguridad en la red Wi-Fi del hogar

Según las declaraciones de los usuarios, sigue aumentando el uso del estándar más seguro de los listados, el WPA2. Esto hace que disminuyan tanto el uso de WPA como el desconocimiento de los usuarios a que este tipo de sistemas protege su red. Sin embargo, según manifiestan los usuarios, el uso de WEP vuelve a aumentar ligeramente.

Cómo configurar tu red Wi-Fi de modo seguro:

https://www.osi.es/es/guia-configuracion-router



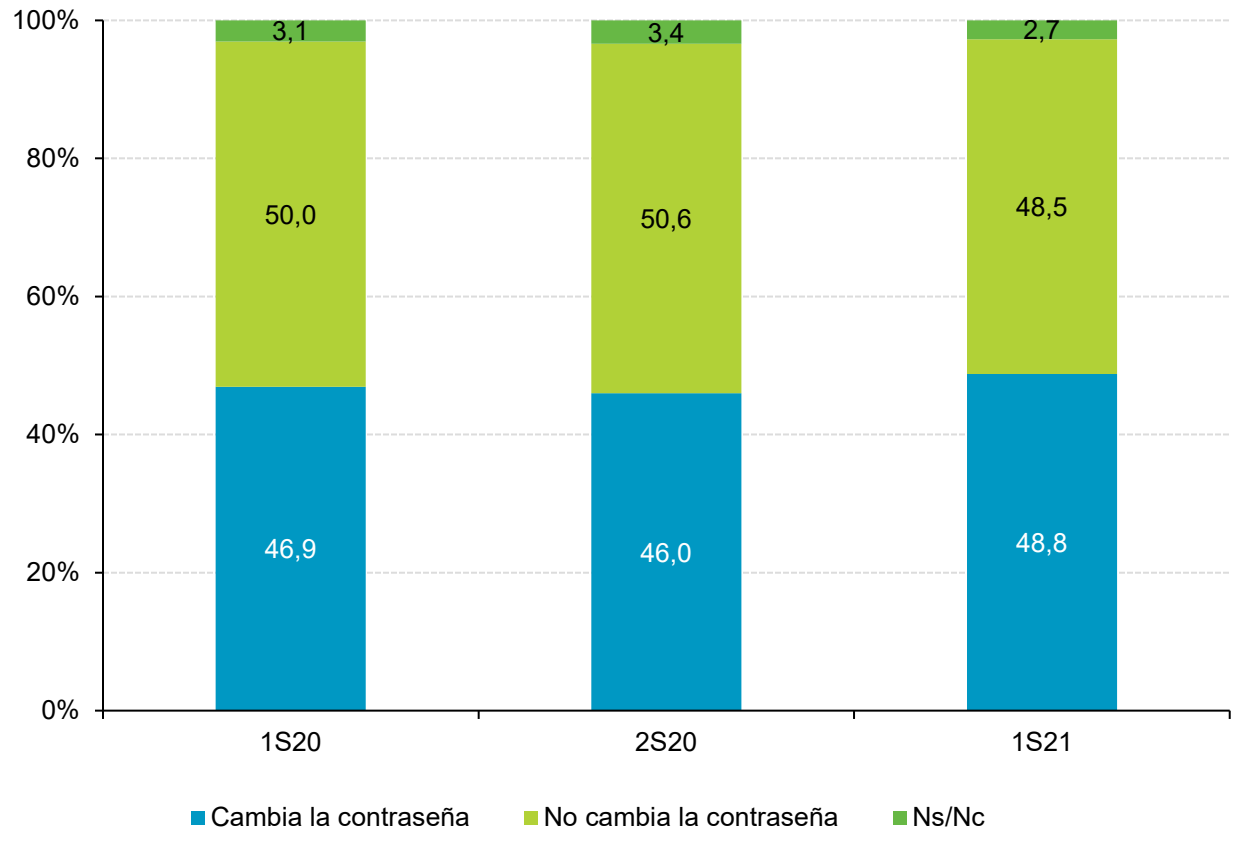
BASE: Usuarios con conexión Wi-Fi propia

Módulo VI: Seguridad en Wi-Fi

Modificación de la contraseña por defecto de la conexión Wi-Fi

El aumento de usuarios que revelan que cambian la contraseña de su propia wifi por defecto es el mayor de los últimos semestres, estando 2,8p.p. por encima del semestre anterior.

Esto provoca una disminución en el porcentaje de los que no cambian la contraseña y de los que desconocen que se pueda cambiar.



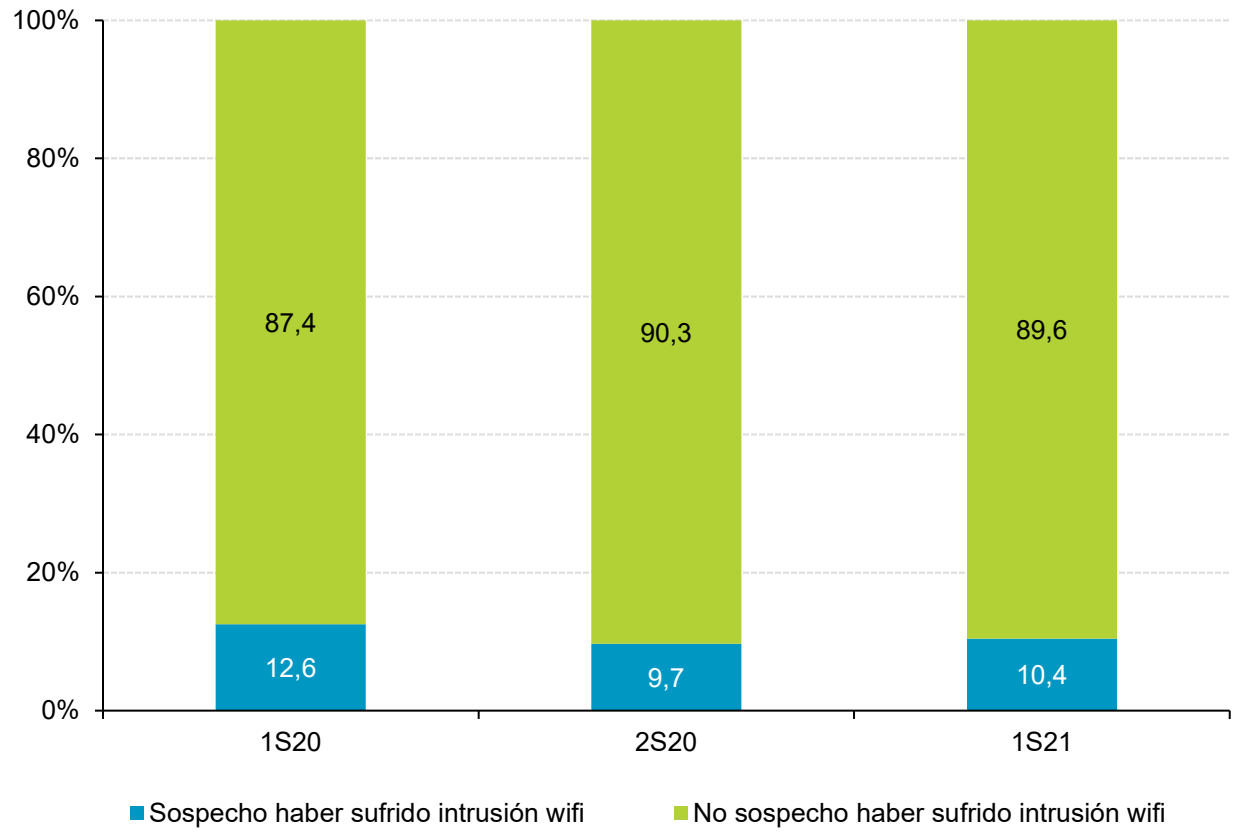
BASE: Usuarios con conexión Wi-Fi propia y sistema de seguridad

Módulo VI: Seguridad en Wi-Fi

Sospecha de haber sufrido una intrusión Wi-Fi (conexión a la red Wi-Fi sin consentimiento)

El 10,4% de los usuarios sospechan haber sufrido una intrusión Wi-fi. Esto supone un leve aumento respecto al semestre anterior, que, además, explicaría el aumento de los usuarios que declaran que ven necesario cambiar la contraseña del router doméstico.

¿Sabes cómo averiguar si alguien está conectado a la red inalámbrica Wi-Fi de tu hogar, cómo actuar al respecto, y como proteger la red para evitarlo?
https://www.osi.es/es/actualidad/blog/2019/09/25/descubre-y-elimina-los-intrusos-de-tu-red-wifi



BASE: Usuarios con conexión Wi-Fi propia

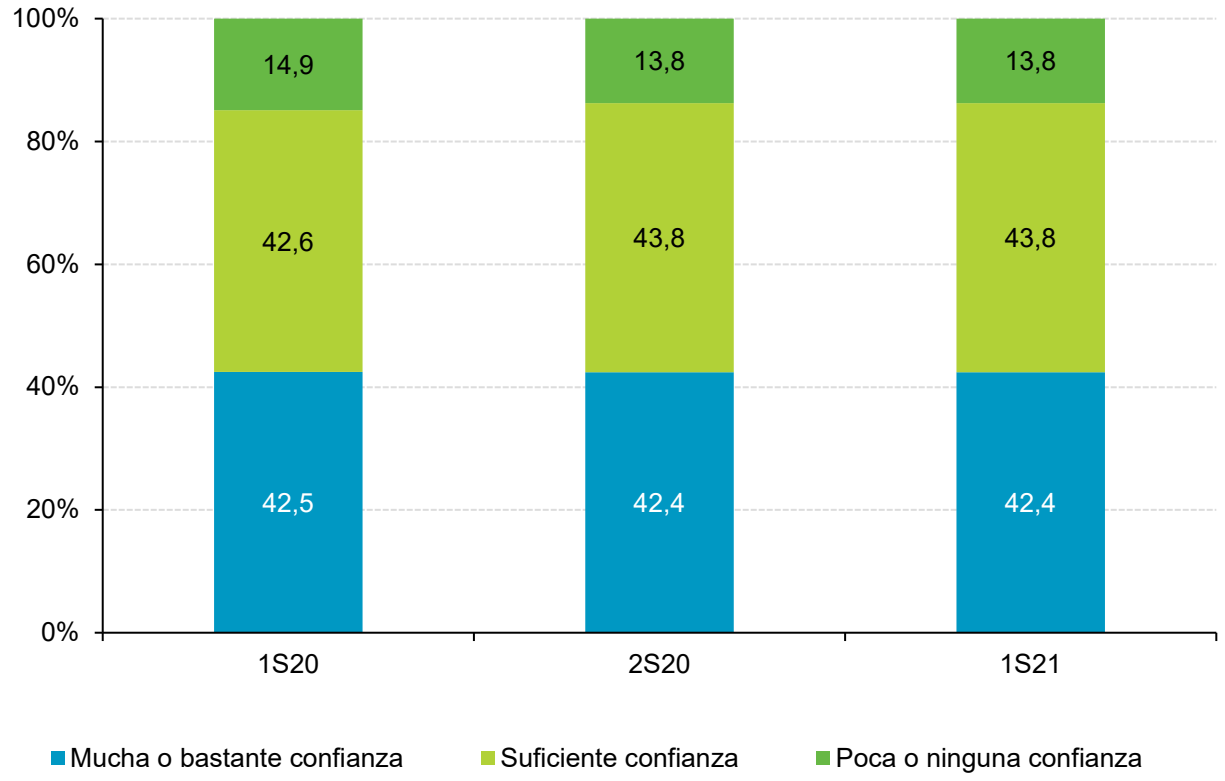
Módulo VII:
Opinión

Módulo VII: Opinión

Nivel de confianza en Internet

En este semestre, según las declaraciones de los usuarios, no ha habido ningún cambio significativo sobre el nivel de confianza en Internet.

Los valores se mantienen iguales respecto al semestre anterior. Más del 80% de los usuarios confían en Internet.



BASE: Total usuarios

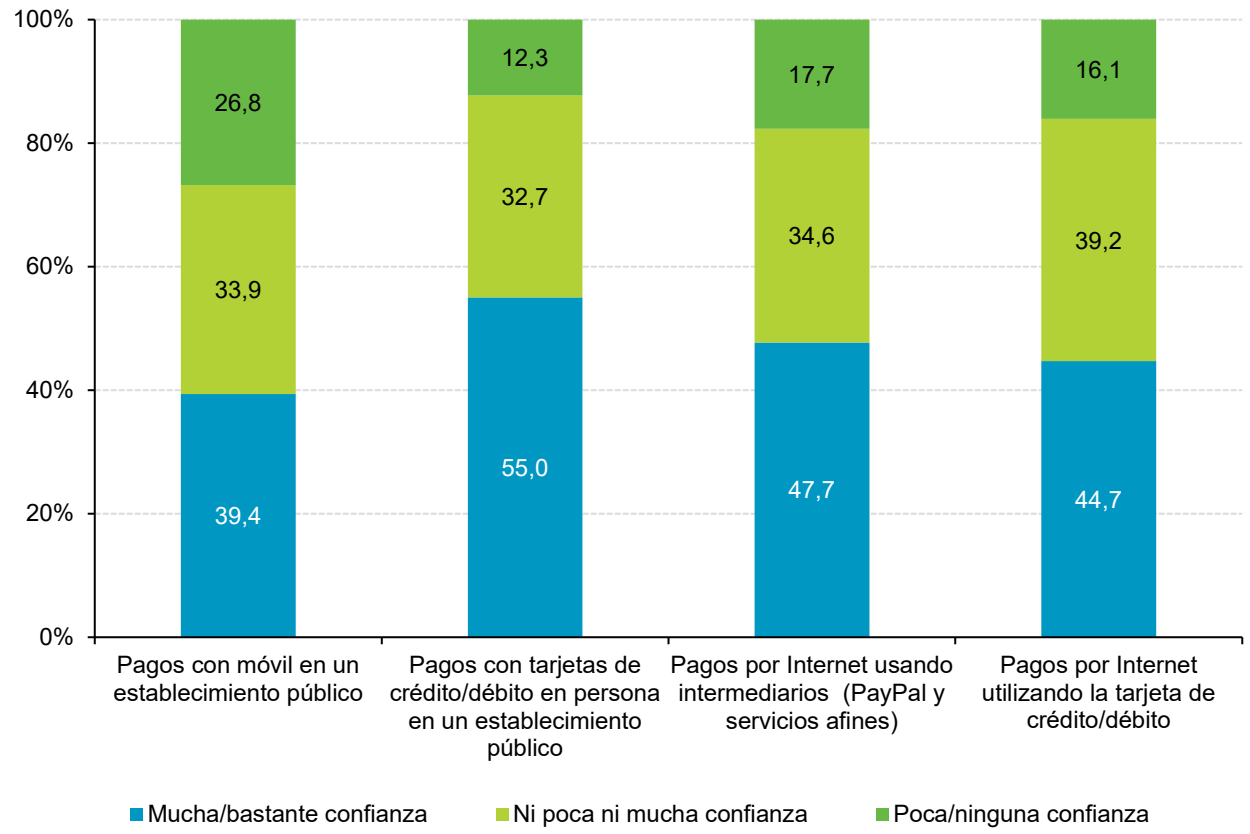
Módulo VII: Opinión

Nivel de confianza al realizar pagos (online y offline)

En este semestre, más de la mitad de los usuarios, en concreto el 55%, aseguran tener mucha confianza en la realización de pagos con tarjetas de crédito en establecimientos públicos.

No se observan grandes variaciones en las declaraciones de los usuarios respecto al uso de servicios como PayPal o las tarjetas de crédito o débito para compras por Internet, cuyos porcentajes continúan por debajo del 50%.

¿Sabes qué precauciones debes tener en cuenta para evitar caer en un engaño al realizar compras online?
https://www.osi.es/es/campanas/compras-seguras-online



BASE: Total usuarios

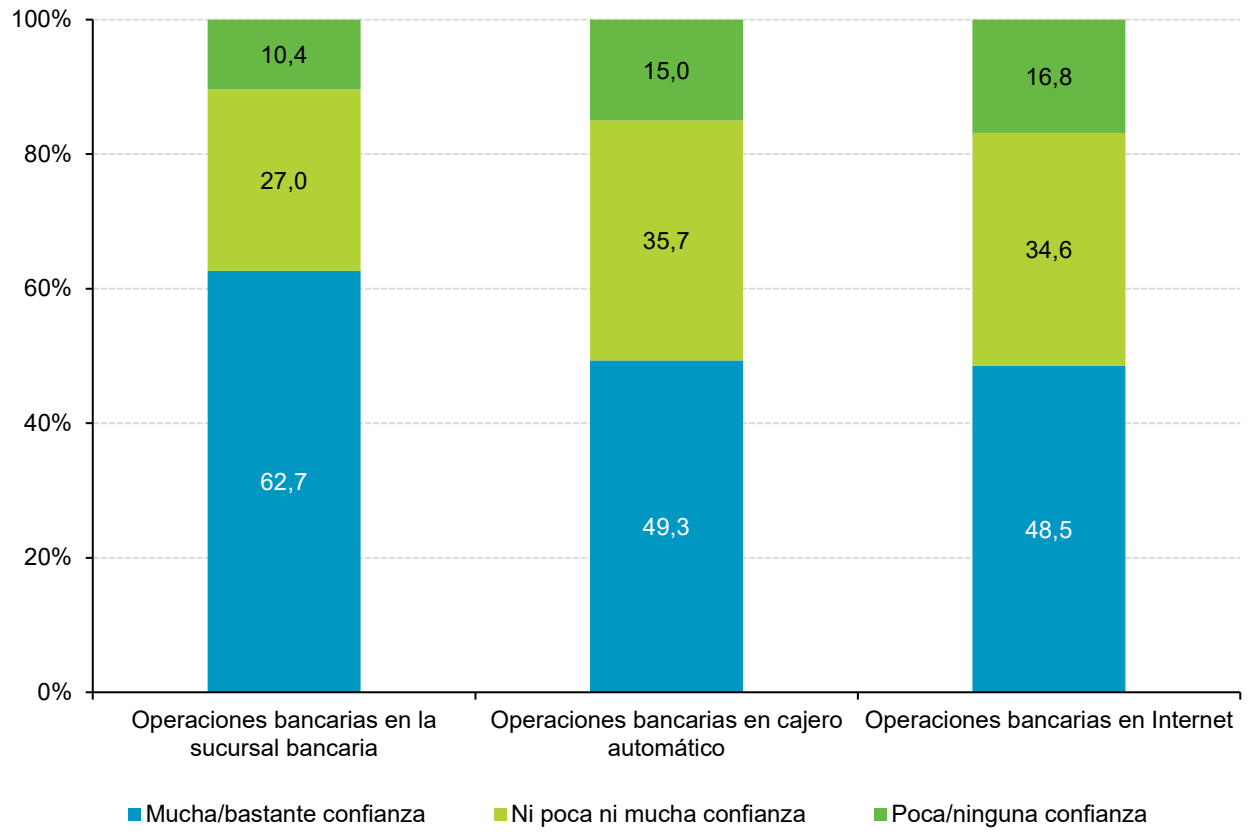
Módulo VII: Opinión

Nivel de confianza al realizar operaciones bancarias (online y offline)

Pese a que la preferencia declarada por los usuarios en este semestre sigue siendo realizar las operaciones bancarias físicamente en su sucursal, el 48,5% de los usuarios manifiestan realizar operaciones bancarias de manera online.

¿Conoces la importancia de tener contraseñas seguras?

https://www.osi.es/es/campanas/contrasenas-seguras



BASE: Total usuarios

Módulo VII: Opinión

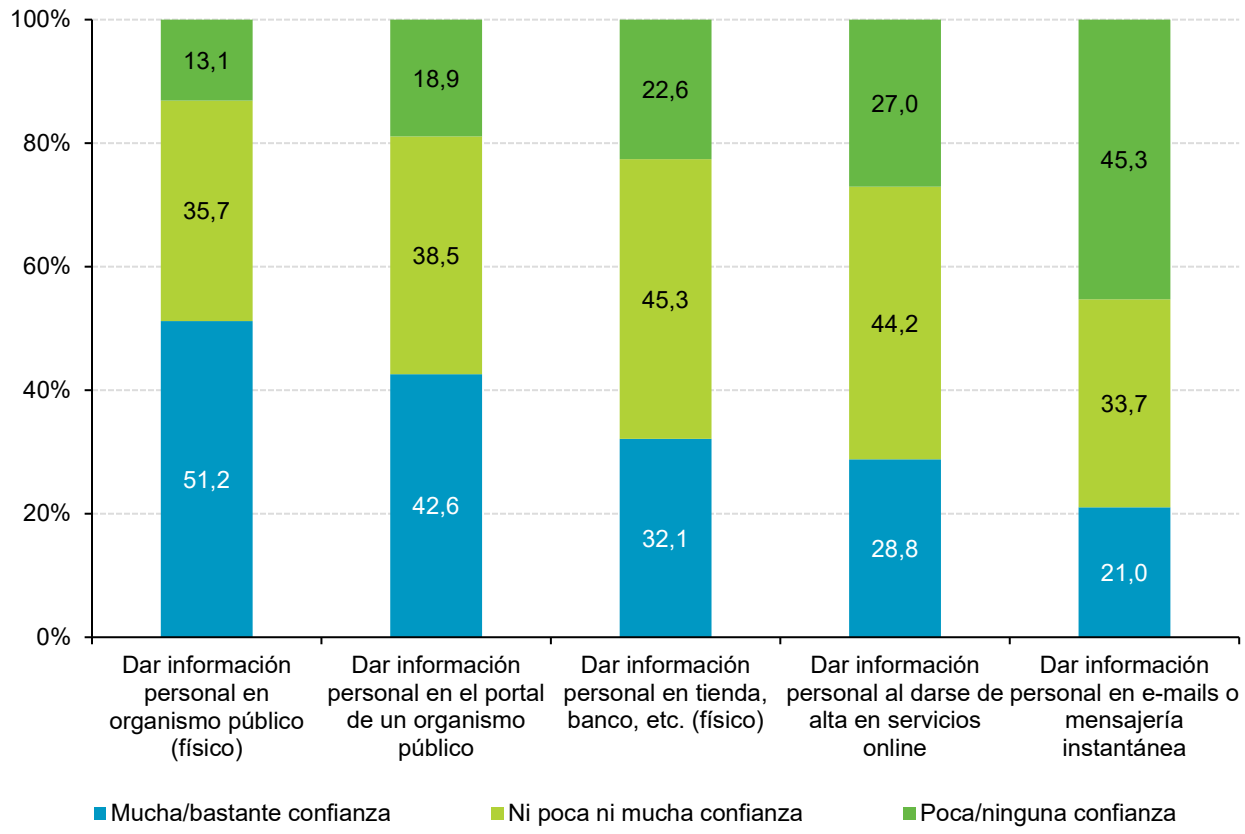
Nivel de confianza al facilitar información personal
(online y offline)

El 51,2% de los usuarios tienen mucha o bastante confianza para dar información personal (en físico) a organismos públicos. El porcentaje desciende al 42,6% en el caso de que la información personal se facilite a través de un portal online.

Cada vez los usuarios parecen estar más concienciados sobre los peligros de dar información personal por email o mensajería instantánea, se puede ver reflejado en las declaraciones de los usuarios recogidas en este último semestre, donde el 45,3% manifiesta que no le inspira confianza compartir información personal por esos medios.

¿Sabes cuánto valen tus datos en la red?

https://www.osi.es/es/cuanto-valen-mis-datos-en-la-red



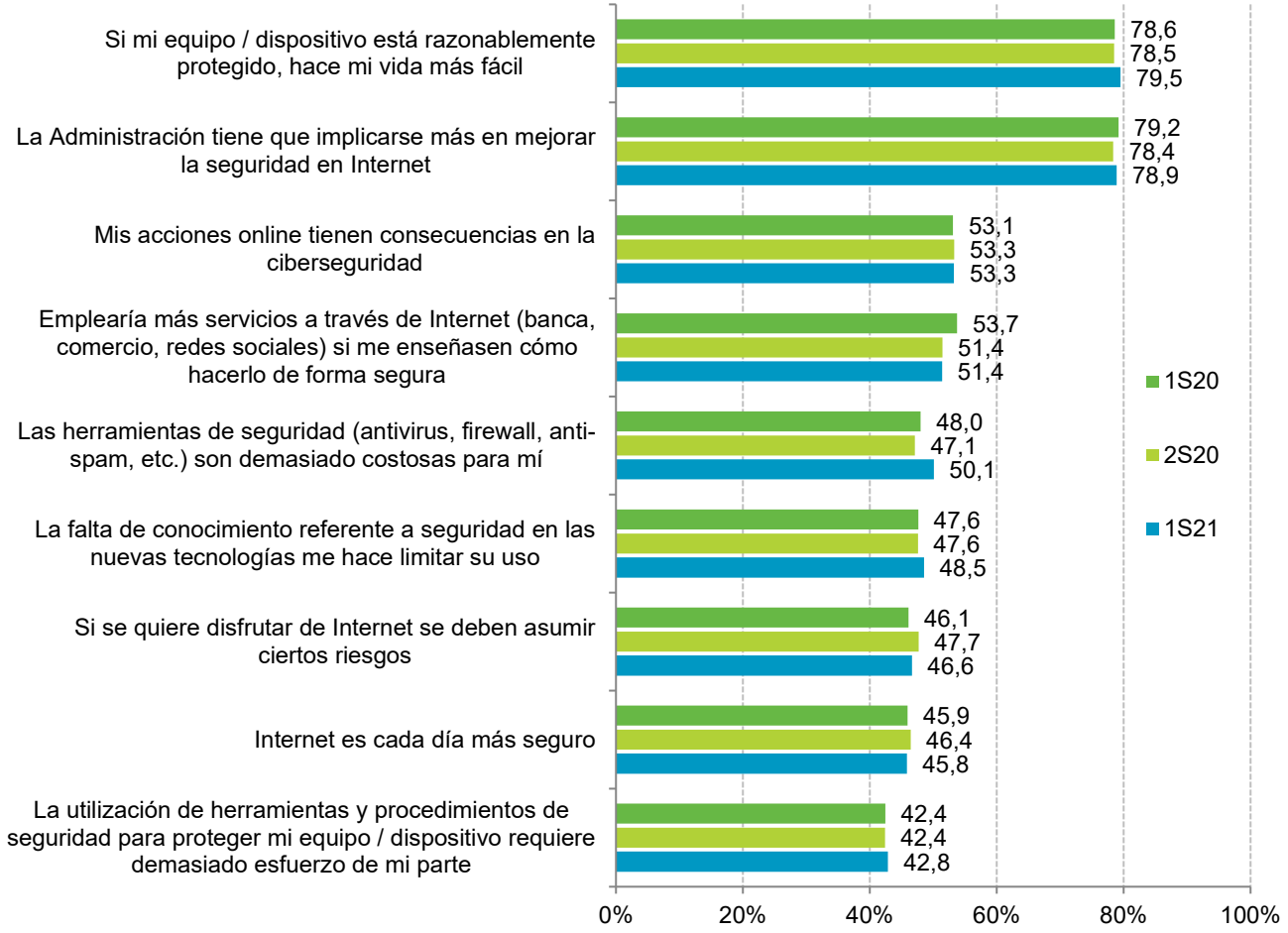
BASE: Total usuarios

Módulo VII: Opinión

Opiniones sobre la seguridad en Internet
(de acuerdo o totalmente de acuerdo)

El 50,1% de los usuarios manifiesta que las herramientas de seguridad como antivirus, firewall, anti-spam, etc. les resultan demasiado costosas. Esa creencia ha aumentado 3 p.p. respecto al semestre anterior.

Se ve un aumento de 1 p.p. de los usuarios que declaran que la falta de conocimientos sobre seguridad en las nuevas tecnologías limita su uso, acercándose al 50% del total de los usuarios entrevistados.



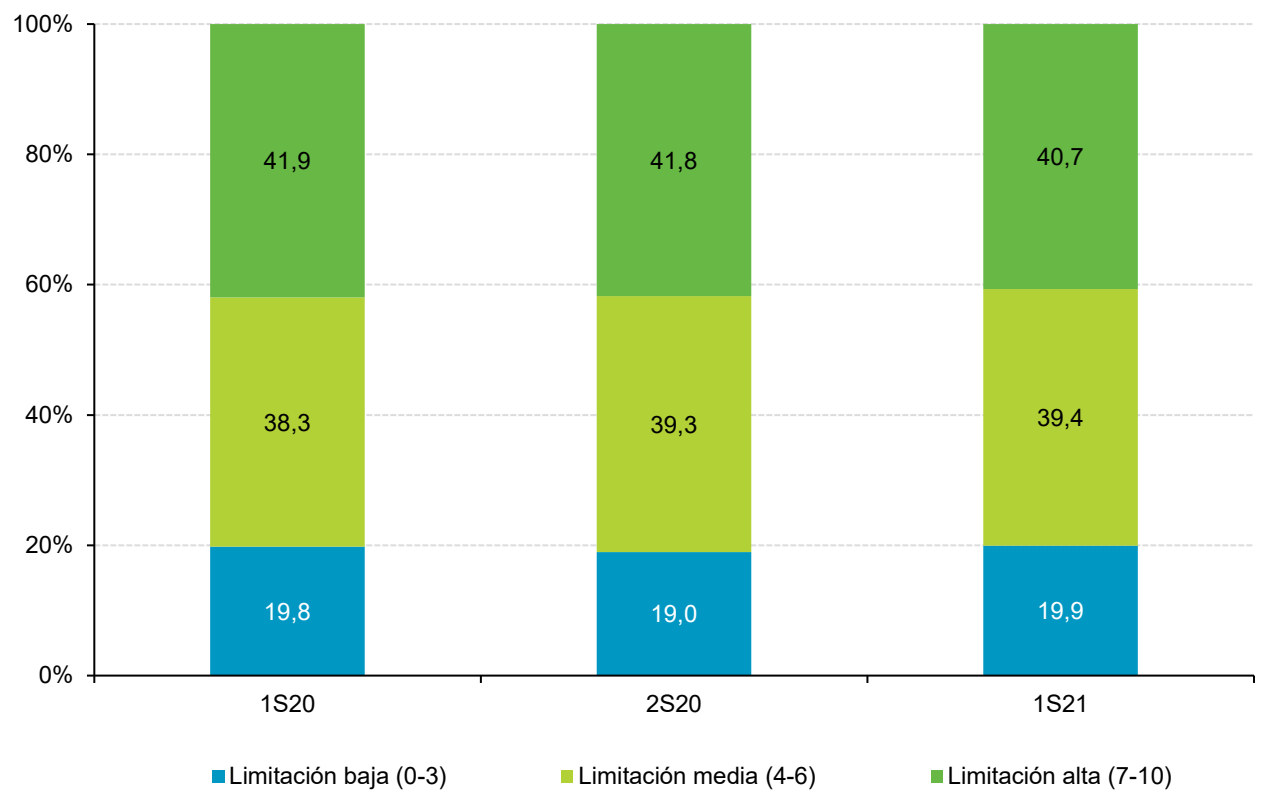
BASE: Total usuarios

Módulo VII: Opinión

Seguridad como factor limitante en la utilización de nuevos servicios en Internet

Por tercer semestre consecutivo, desciende el número de usuarios que declara percibir la seguridad como un factor altamente limitante en el uso de nuevos servicios.

Sin embargo, el porcentaje de usuarios que considera la seguridad como una limitación media asciende alrededor de 1p.p. en comparación con el semestre anterior.



BASE: Total usuarios

Módulo VII: Opinión

Percepción de los riesgos a los que se está más expuesto al navegar por Internet

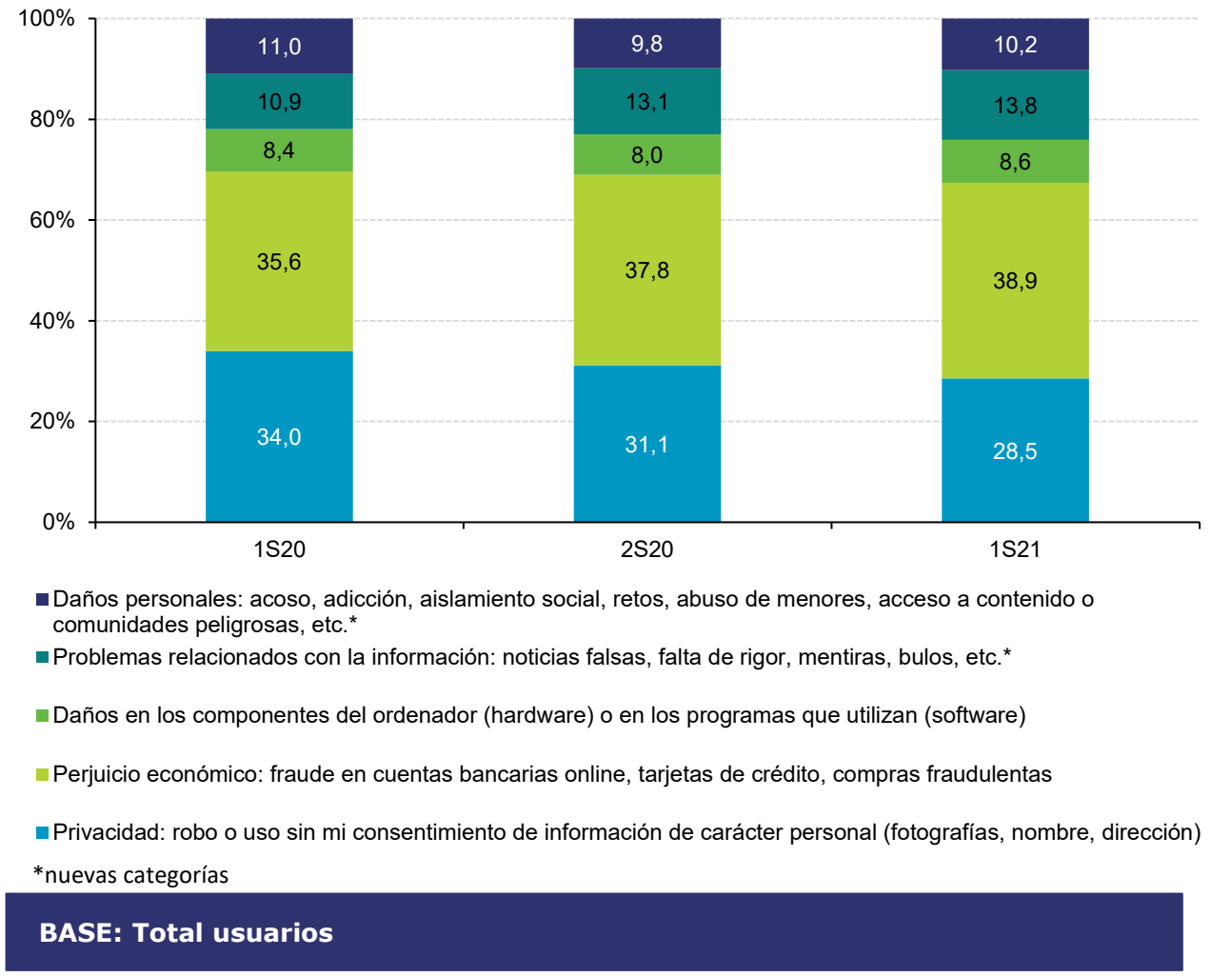
El perjuicio económico ocasionado por fraude sigue siendo la opción que más preocupa, según las declaraciones del 38,9% de los usuarios.

¿Sabes como cuidar tu privacidad en Internet y tus datos en la nube?

✓ ***Borra tu huella:*** *https://www.youtube.com/watch?v=FT1FjR1XQ2w&feature=youtu.be*

✓ ***Cómo disminuir tu rastro en Internet:*** *https://www.osi.es/es/como-disminuir-tu-rastro-en-internet*

✓***Ejerciendo el "derecho al olvido":*** *https://www.osi.es/es/actualidad/historias-reales/2020/11/04/ejerciendo-el-derecho-al-olvido*



*nuevas categorías

BASE: Total usuarios

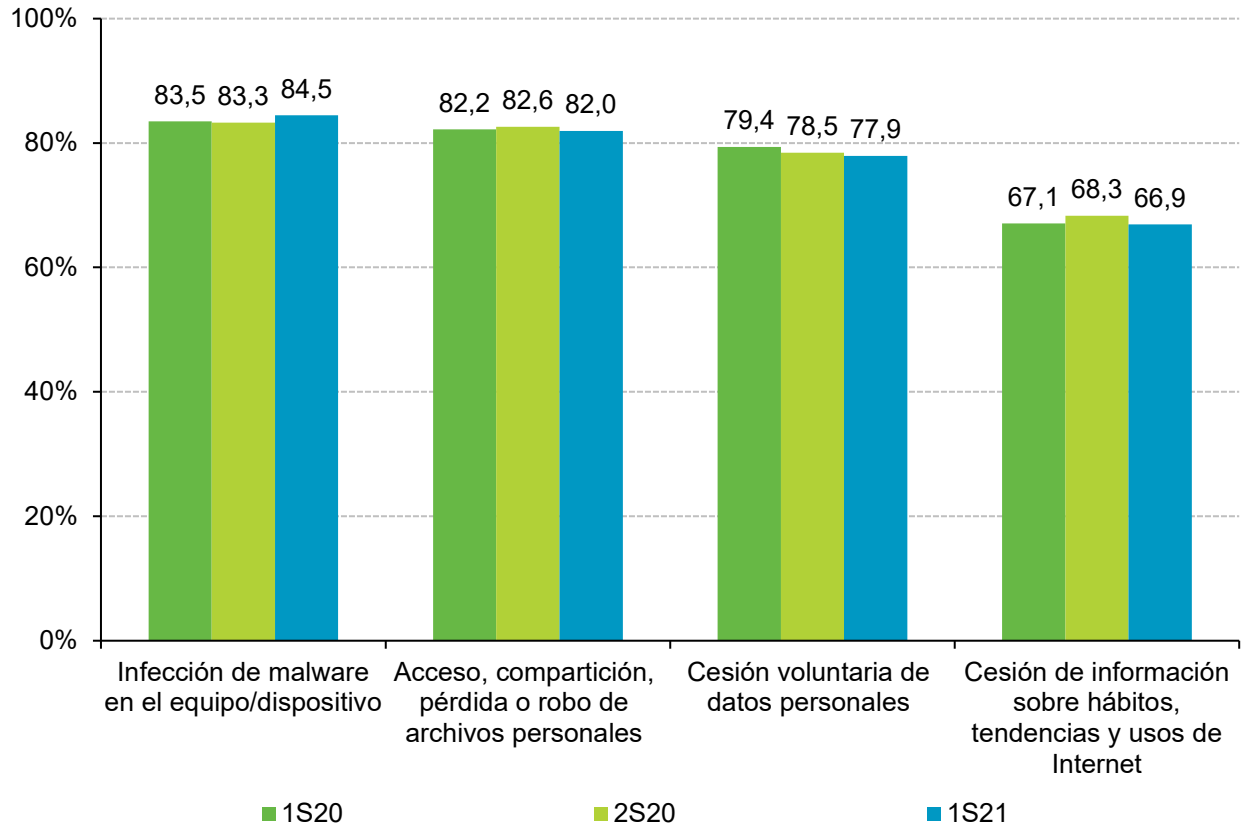
Módulo VII: Opinión

Valoración de los peligros al navegar por Internet

(bastante o muy importante)

Según declaran los panelistas, el 84,5% valora como más peligrosa la infección de *malware* en su equipo o dispositivo.

Continúa disminuyendo progresivamente el porcentaje de usuarios que ceden de manera voluntaria sus datos personales.



BASE: Total usuarios

Módulo VIII:

Datos reales procedentes de los análisis realizados por Pinkerton

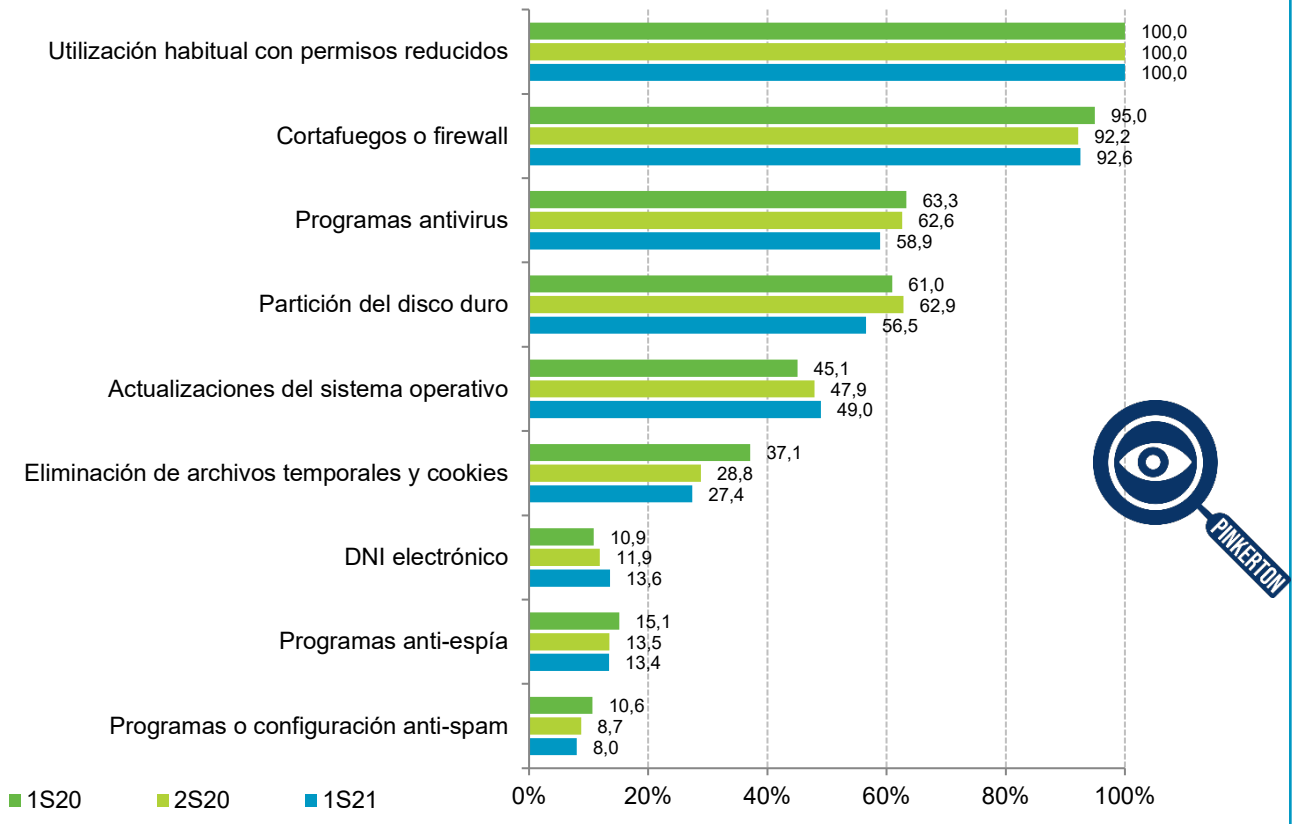
Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Uso real de medidas de seguridad en el ordenador del hogar

Sigue en aumento el porcentaje de usuarios de PC que tienen el sistema operativo actualizado. Además, se detecta también un aumento de 1,7 p.p. del uso del DNI electrónico sobre los datos obtenidos en el semestre anterior.

En contraposición, cabe destacar que ha disminuido 6,4 p.p. el porcentaje de usuarios de PC cuyos equipos tienen particionado el disco duro.

Utiliza la cuenta de usuario estándar para el uso diario del ordenador, dejando la cuenta de administrador sólo para cuando sea estrictamente necesario. Más información sobre las cuentas de usuario y cómo configurarlas en: https://www.osi.es/cuentas-de-usuario

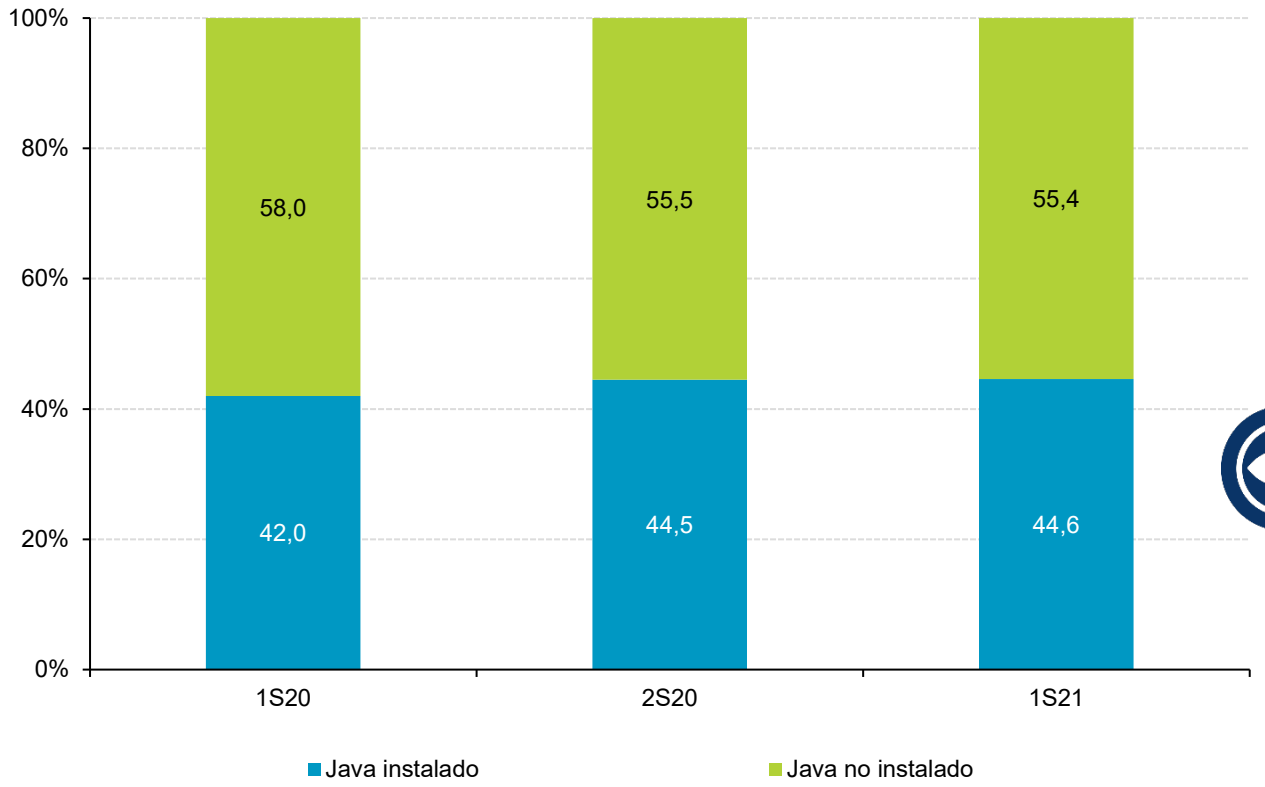


Base: Usuarios de PC

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Entorno Java en el ordenador del hogar

La variación del porcentaje de usuarios con dispositivos que tienen java instalado no resulta significativa, aunque aumenta con respecto al semestre anterior.



El aprovechamiento y explotación de vulnerabilidades en Java ha sido, a lo largo de los últimos años, uno de los vectores de entrada más utilizados por el *malware* para infectar equipos con una versión de este *software* desactualizada.

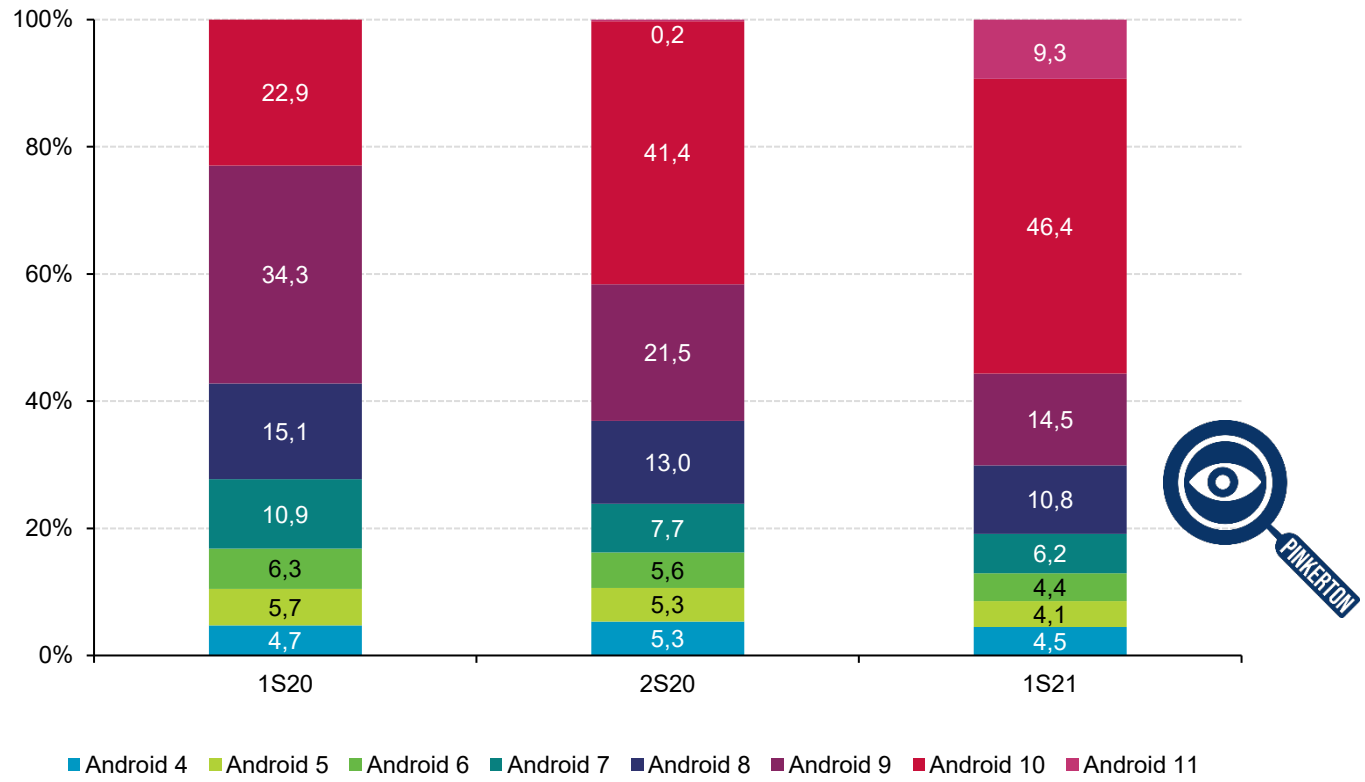
Base: Usuarios de Microsoft Windows

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Versiones de Android

El porcentaje de usuarios con Android 10 aumenta 5 p.p. respecto al semestre anterior, pese a estar disponible desde septiembre de 2020 la versión de Android 11.

Igualmente, se experimenta un incremento de 9,1 p.p en el porcentaje de usuarios de dispositivos Android 11. Se puede observar que las versiones anteriores a la de Android 10, cada vez son menos utilizadas.



Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Uso real de medidas de seguridad en dispositivos Android

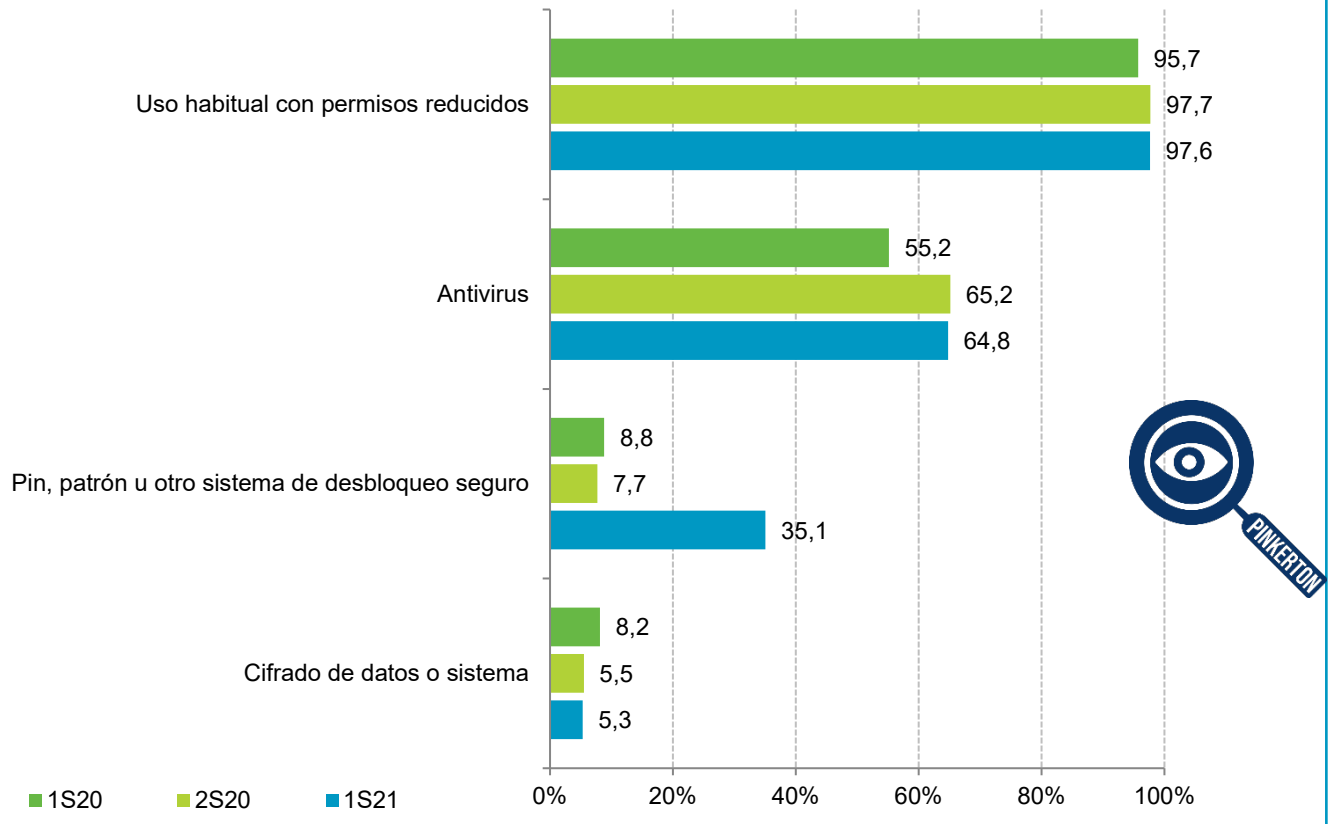
Cabe destacar que en este semestre se ha observado un aumento significativo de usuarios que utilizan alguna medida de desbloqueo seguro en su dispositivo Android. El 35,1% usa alguno de esos sistemas frente al 7,7% del semestre anterior.

*La utilización de un sistema de desbloqueo seguro mediante **patrón, PIN, sistemas biométricos**, etc., permite evitar de manera sencilla los **accesos no autorizados o no deseados** al dispositivo móvil y su contenido, **protegiendo la privacidad del usuario**.*

Más información:

https://www.osi.es/es/actualidad/blog/2020/10/23/bloquear-dispositivo-android-ios-biometria

https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas



Base: Usuarios de dispositivos Android

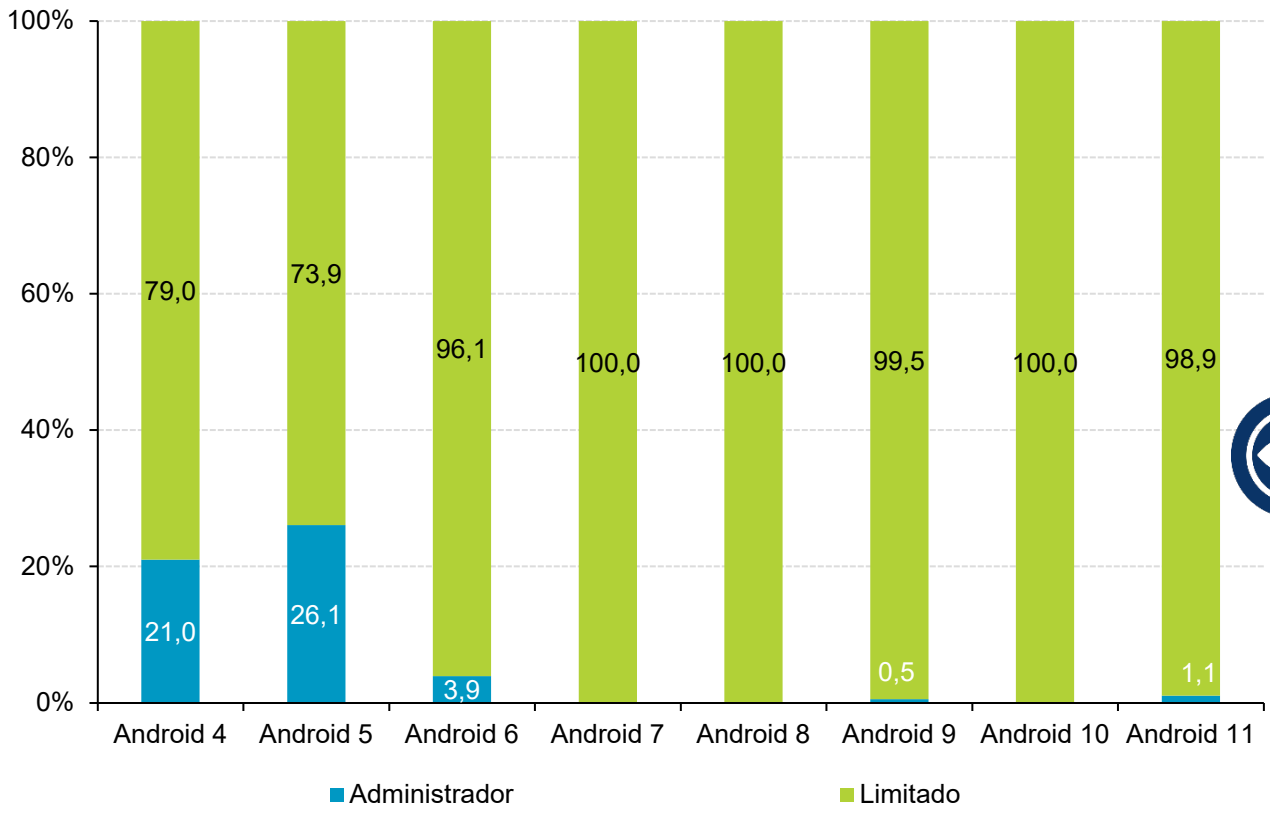
Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Nivel real de privilegios en los perfiles de usuario de dispositivos Android

Se puede observar que a partir de la versión de Android 7 el nivel de permisos de los usuarios es limitado. Esta es una de las características más significativas en las últimas oleadas.

Guía para configurar dispositivos móviles: Más información:

https://www.osi.es/es/guia-para-configurar-dispositivos-moviles

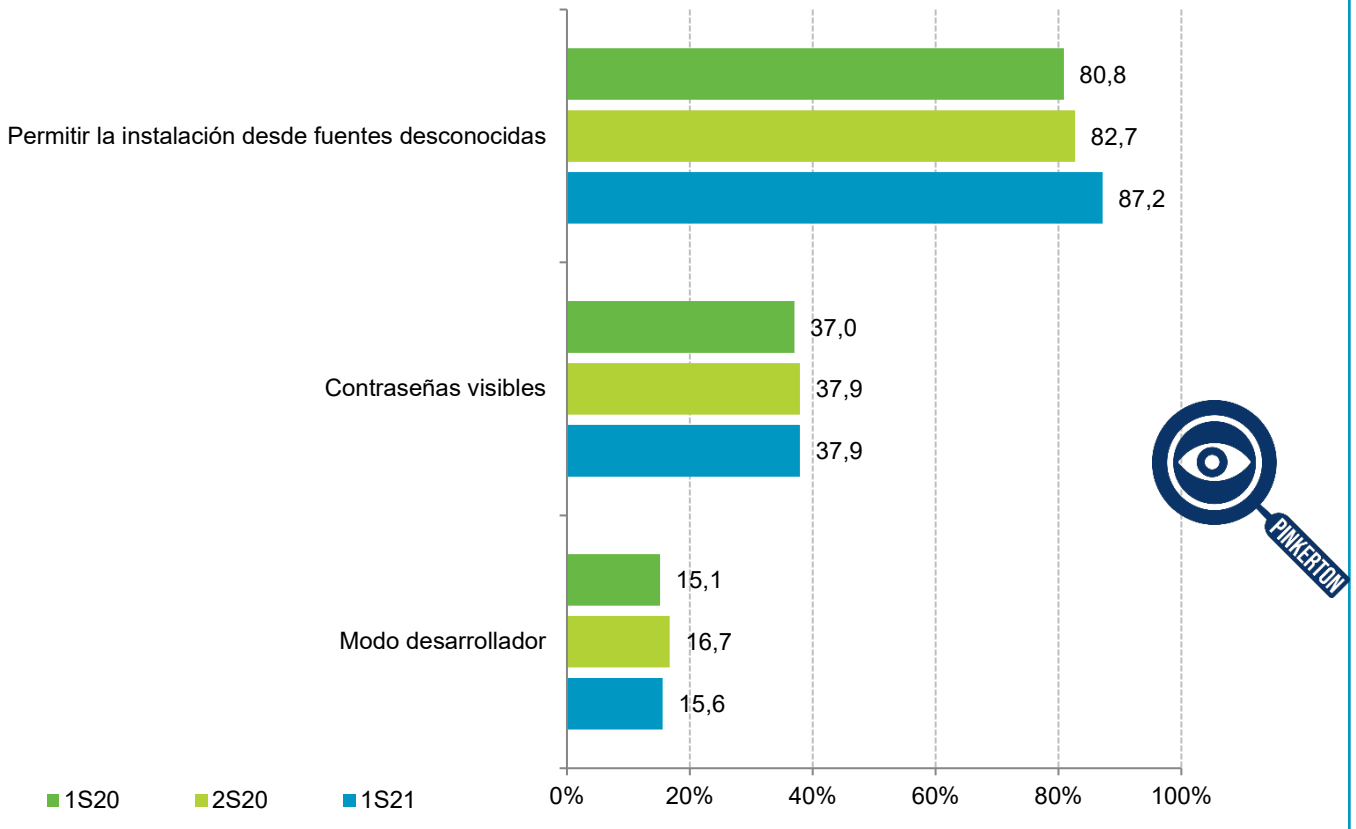


Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Configuraciones activas en dispositivos Android

Se está extendiendo el hábito de utilizar fuentes desconocidas para las descargas. Se ha obtenido el valor más alto de las tres últimas oleadas, el 87,2% de los usuarios tienen activa esta característica en la configuración de su dispositivo Android.



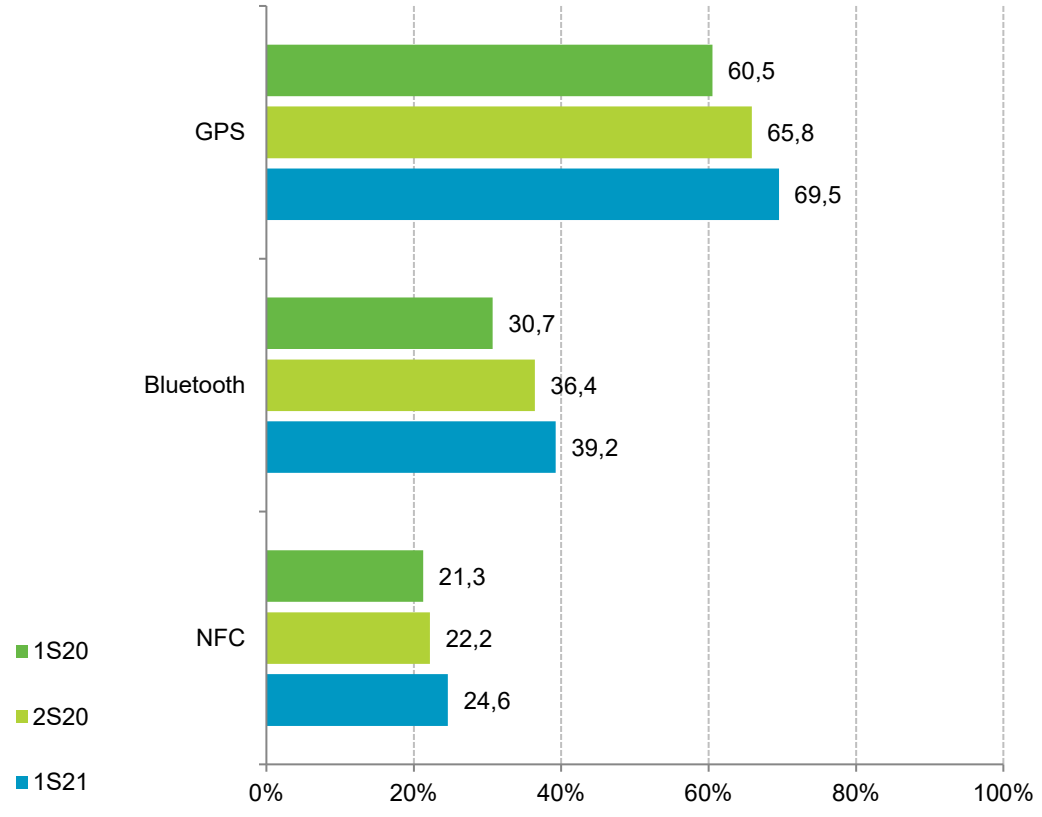
Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Tecnologías activas en dispositivos Android

El uso del GPS vuelve a ser el más destacado entre las tecnologías que tienen activas los usuarios con dispositivos Android, y continúa aumentando sobre la oleada anterior, en esta ocasión 3,7 p.p.

El uso de la tecnología Bluetooth y NFC también es cada vez más popular; como se puede observar, continúa aumentando, aunque más lentamente que el uso del GPS.



Base: Usuarios de dispositivos Android

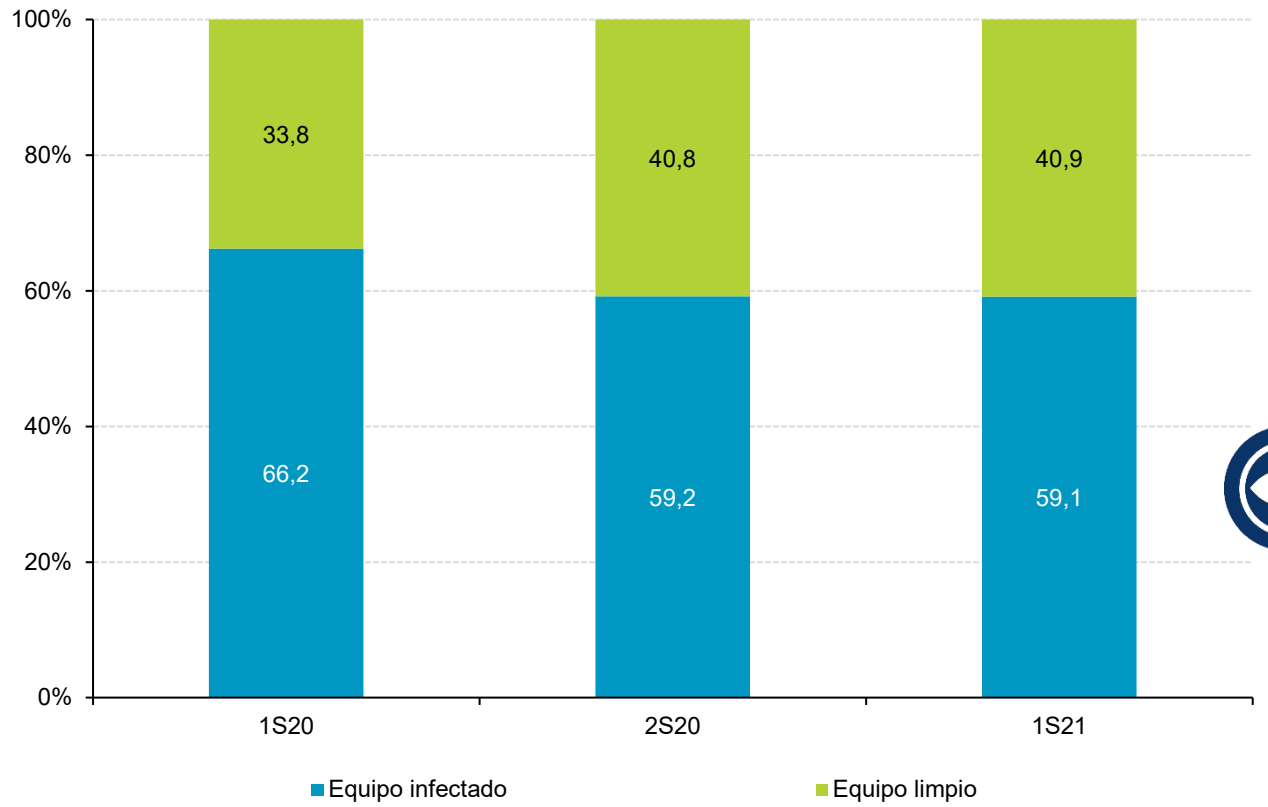
Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Estado de infección real del ordenador del hogar

No hay cambios significativos en cuanto al porcentaje de ordenadores del hogar infectados, ya que prácticamente se mantiene estable con respecto a los datos observados en el semestre anterior, con una diferencia de -0,1p.p.

No obstante, el 59,1% de los equipos escaneados sigue siendo una cifra muy elevada.

Aprende los pasos que debes dar para la eliminación de los virus de tu equipo:
https://www.osi.es/es/desinfecta-tu-ordenador



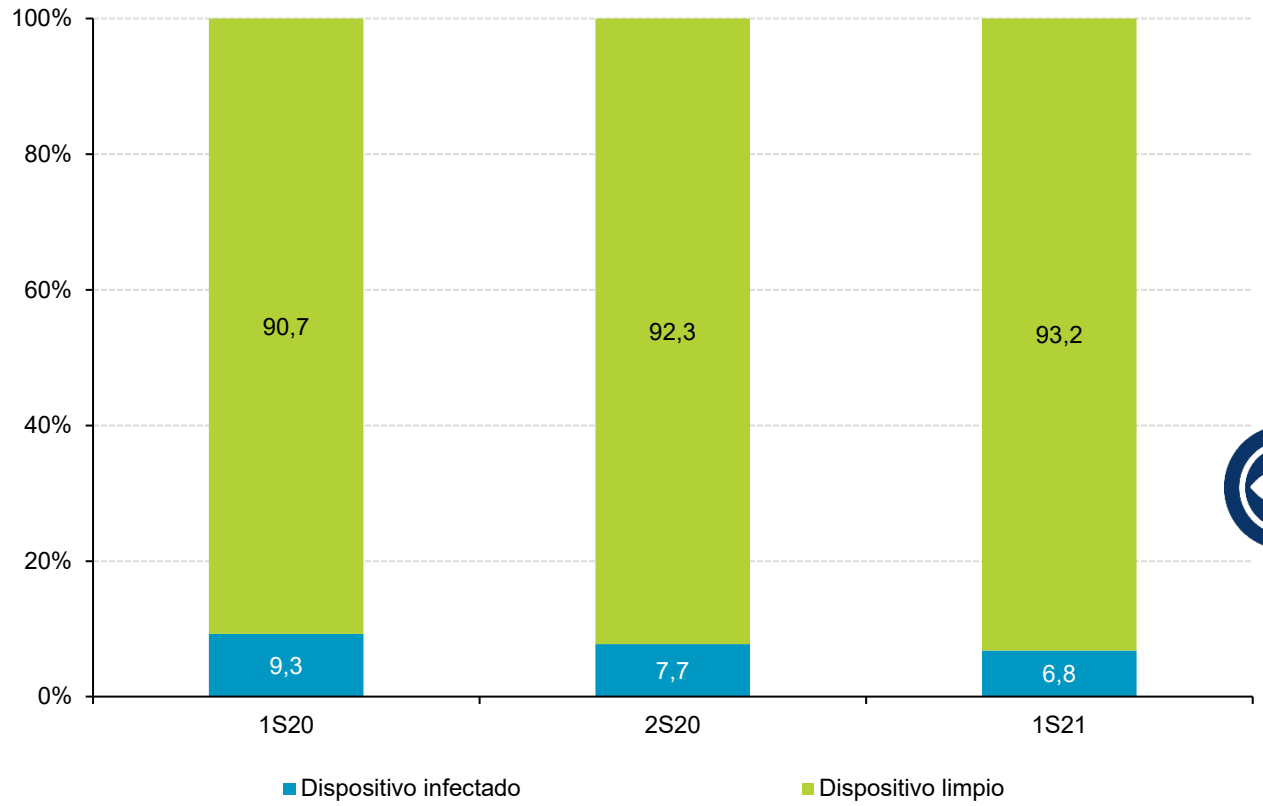
BASE: Total ordenadores

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Estado de infección real de los dispositivos Android

Se registra un descenso en los casos de infecciones por *malware* en dispositivos Android.

Las nuevas versiones de Android, las actualizaciones y el bajo nivel de privilegio de los dispositivos con versiones de Android 7 en adelante, contribuyen en la mejora de la seguridad de los dispositivos.



BASE: Total dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

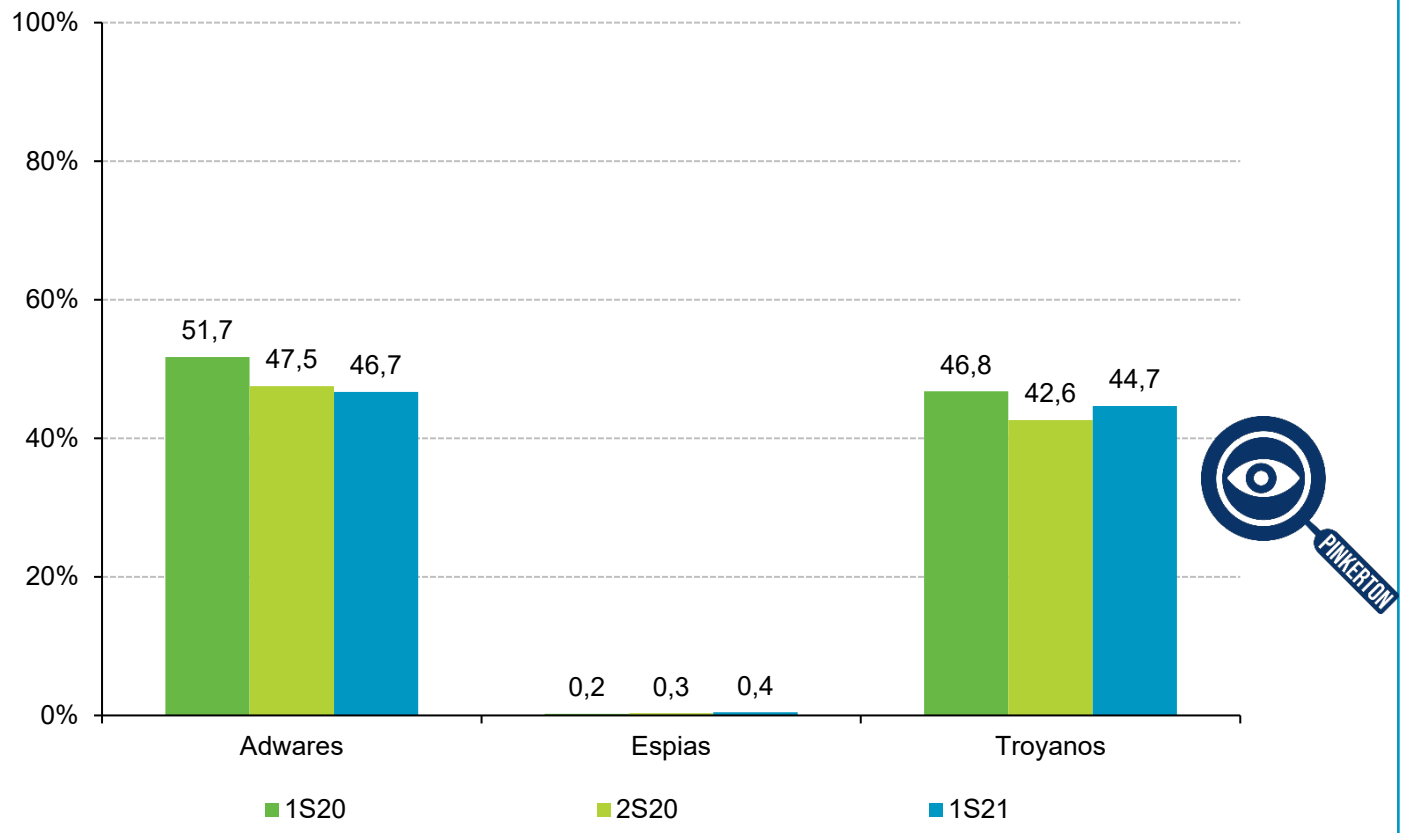
Tipología del *malware* detectado en el ordenador del hogar

Se ha observado un aumento de los troyanos en los ordenadores del hogar analizados de 2,1 p.p. respecto al semestre anterior. Mientras que los *Adwares* disminuyen levemente, se observa que la proporción de *software* espía sigue en aumento, aunque muy paulatinamente.

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Tipos de malware:
https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos

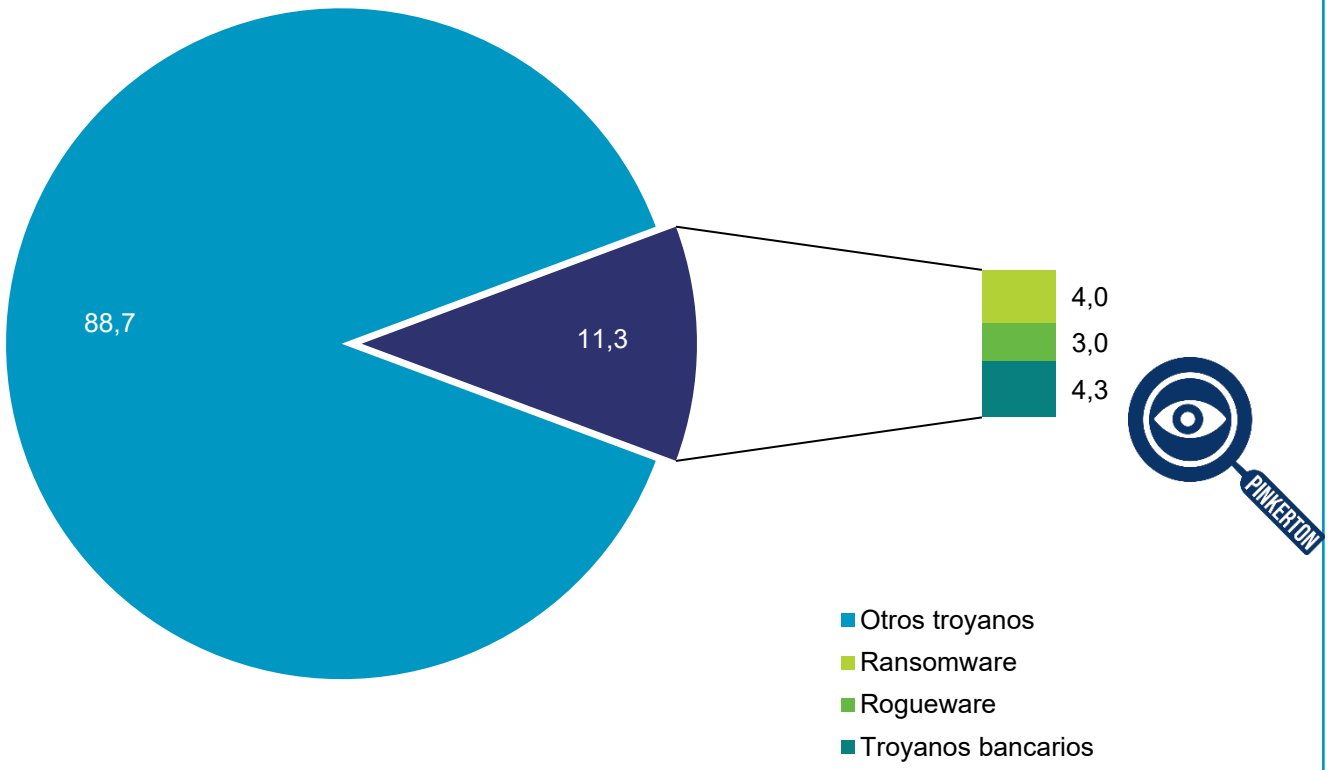


BASE: Total ordenadores

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Clasificación de troyanos detectados en el ordenador del hogar

En el 88,7% de los ordenadores con troyanos detectados se identifican otros troyanos. Por su parte, el 11,3% sufre tres tipos de *malware* vinculados con el fraude (troyanos bancarios, *ransomware* y *rogueware),* siendo los troyanos bancarios y el ransomware los que presentan porcentajes más elevados, 4,3% y 4%, respectivamente.



BASE: Total ordenadores con troyanos detectados

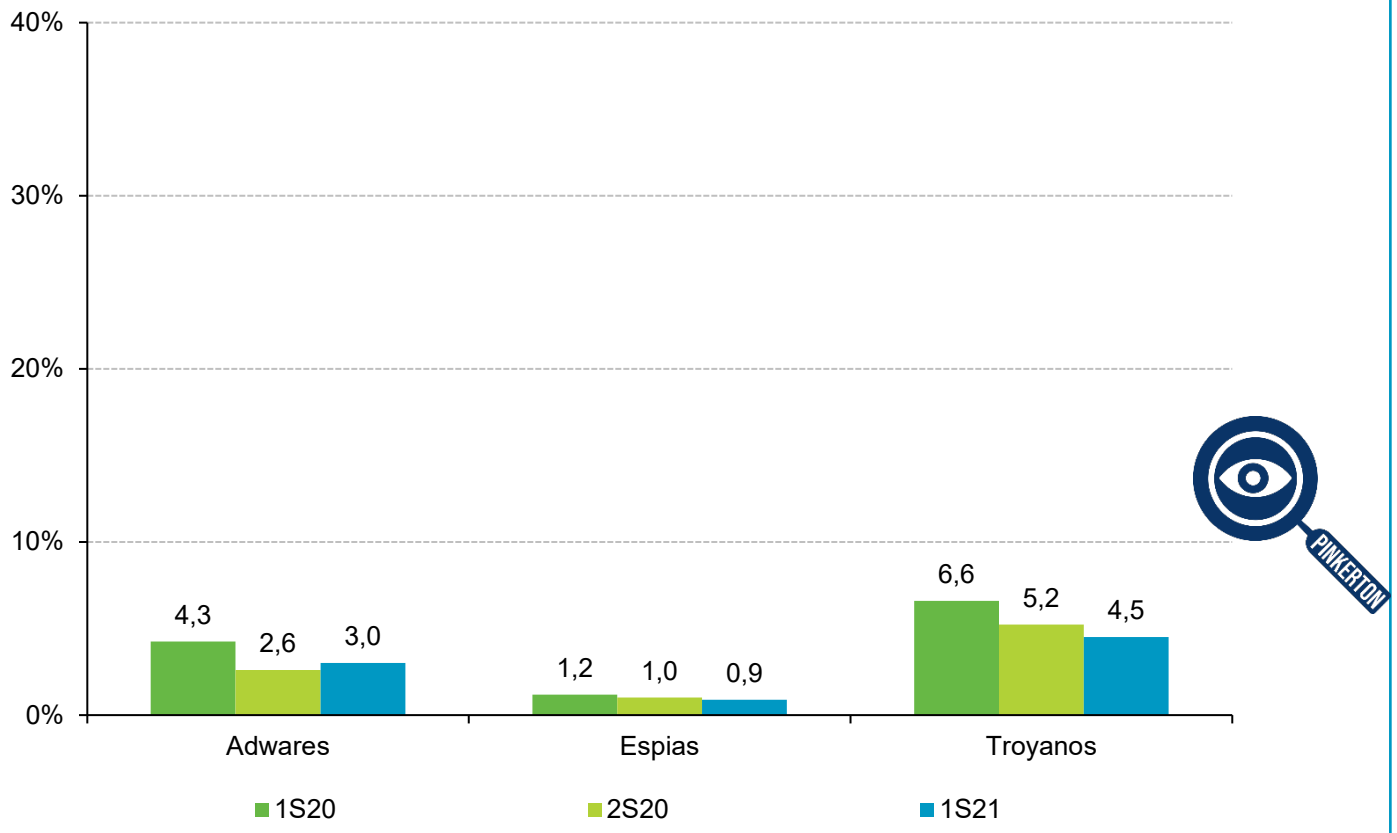
Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Tipología del *malware* detectado en dispositivos Android

Respecto a los semestres anteriores, se percibe un descenso en la infección de los dispositivos por los tipos troyano y espías, mientras que los *adware* aumentan al 3%.

Los troyanos se mantienen como el *malware* más presente en este tipo de plataformas.

Guía de ciberataques:
https://www.osi.es/es/guia-ciberataques



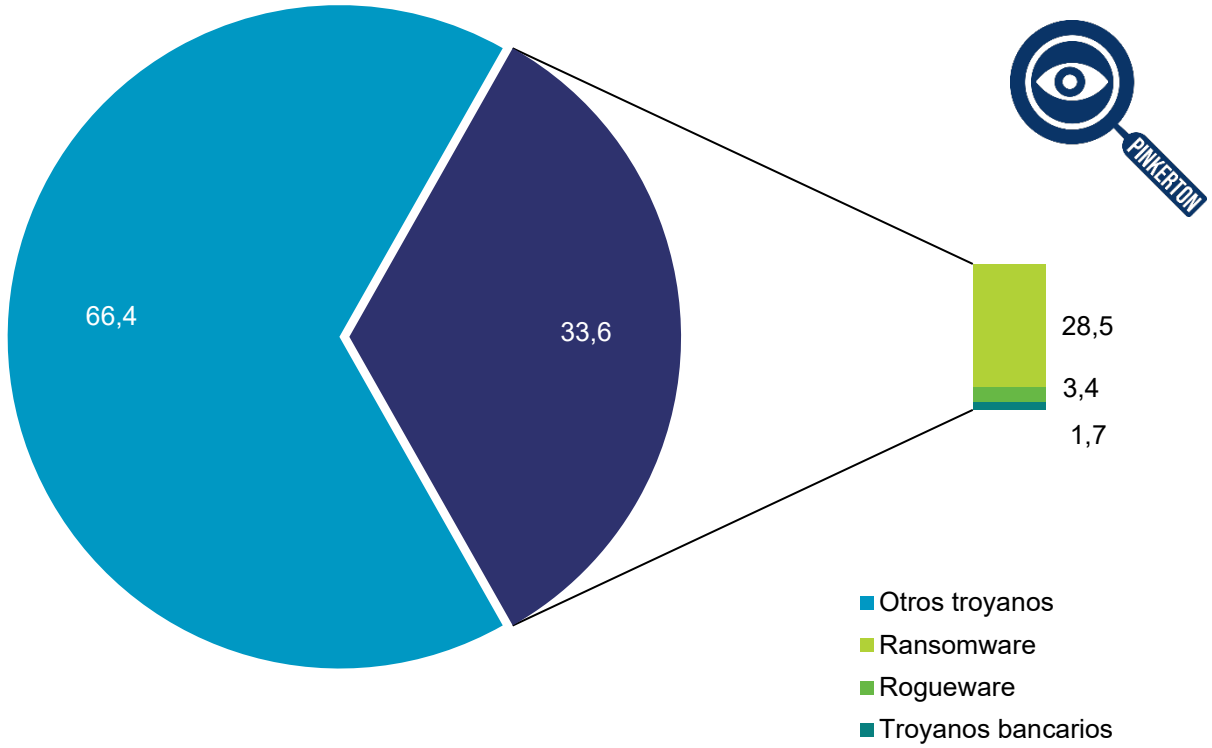
BASE: Total dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Clasificación de troyanos detectados en dispositivos Android

Del total de los troyanos detectados en dispositivos Android, el 33,6% han sido *ransonwares, roguewares* o troyanos bancarios.

El *malware* de tipo *ransomware* (cifrado y secuestro de datos) ocupa el 28,5% seguido por los *rogueware*, situado en el 3,4%.

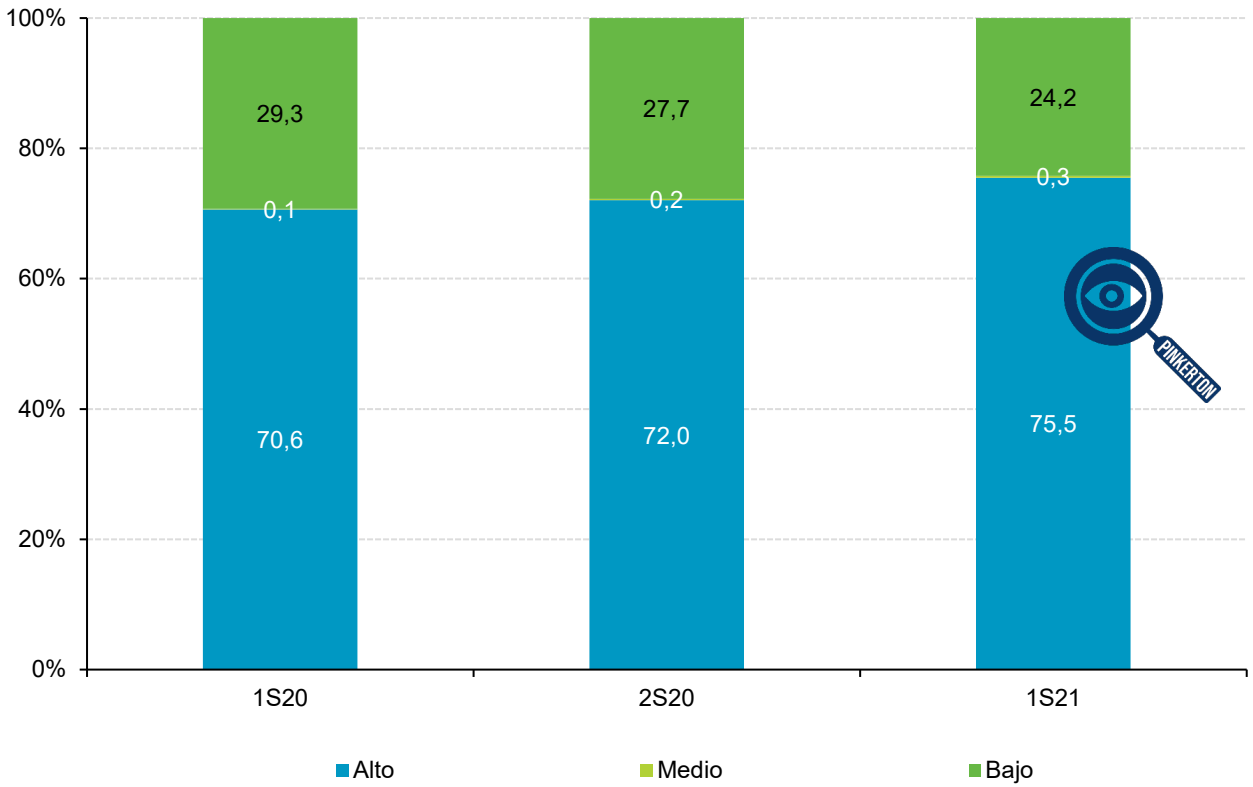


BASE: Total dispositivos Android con troyanos detectados

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Peligrosidad del *malware* detectado y riesgo en el ordenador del hogar

Aumenta 3,5 p.p. la peligrosidad alta del *malware* detectado, ya que en este semestre el 75,5% de los equipos contienen *malware* de peligrosidad alta. También se observa un leve aumento en el *malware* de peligrosidad media.



Nota: la clasificación de peligrosidad del tipo de *malware* se define en la introducción del estudio

BASE: Total ordenadores infectados

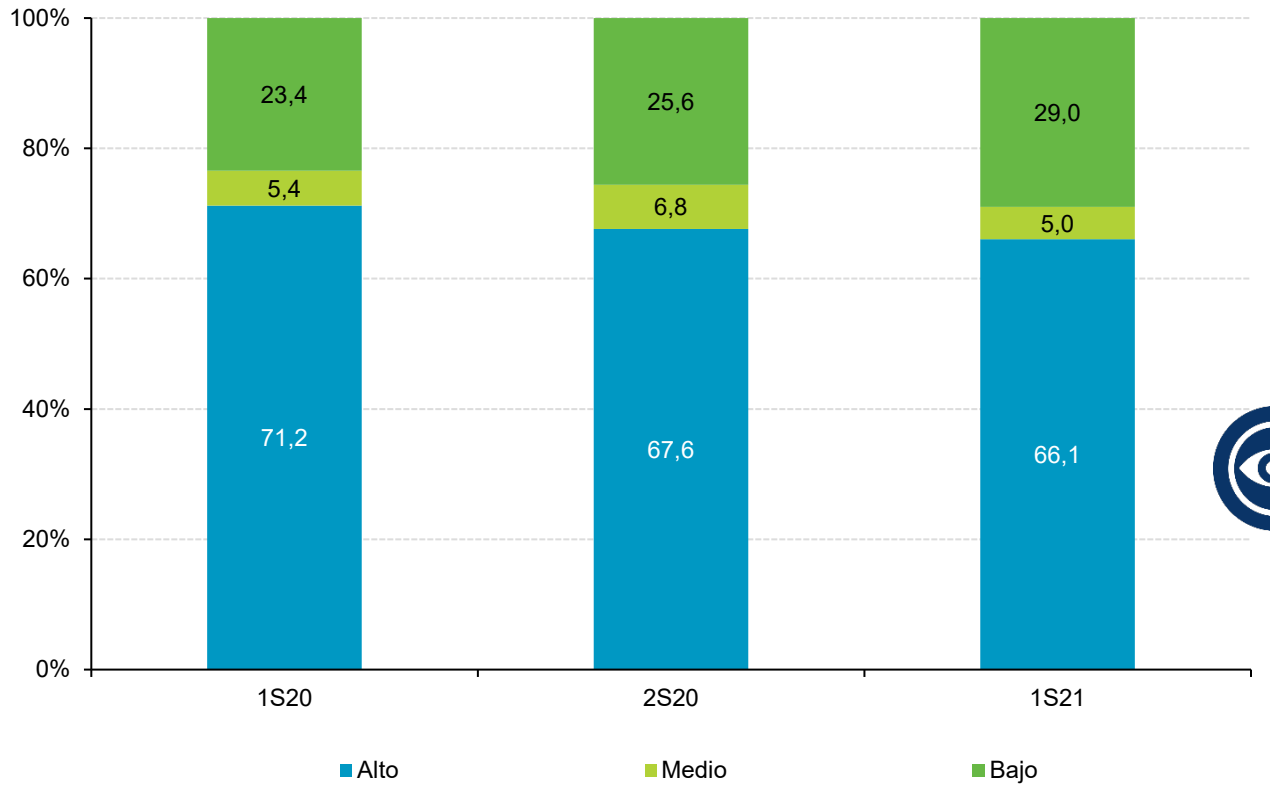
Guía de ciberataques:
https://www.osi.es/es/guia-ciberataques

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Peligrosidad del *malware* detectado y riesgo de los dispositivos Android

Para los dispositivos Android, la peligrosidad sigue bajando este semestre. El 66,1% de estos equipos se encuentran infectados con *malware* de peligrosidad alta, 1,5 p.p. menos que el porcentaje del semestre anterior. En cambio, se ha observado que los dispositivos Android infectados con *malware* de peligrosidad media se hacen notar más que en el caso de los ordenadores, siendo del 5,0%.

Tipos de malware:
https://www.osi.es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus



Nota: la clasificación de peligrosidad del tipo de *malware* se define en la introducción del estudio

BASE: Total Dispositivos Android infectados

Alcance del estudio

Alcance del estudio

El "*Estudio sobre la Ciberseguridad y Confianza del ciudadano en la Red",* se realiza a partir de una metodología basada en el panel online dedicado y compuesto por aquellos hogares con conexión a Internet repartidos por todo el territorio nacional.

Los datos extraídos de la encuesta, realizada con una periodicidad semestral, permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios.

Ficha técnica

Universo: Usuarios españoles de Internet mayores de 15 años con acceso a Internet desde el hogar (al menos una vez al mes).

Tamaño Muestral: 3.711 hogares encuestados y equipos/dispositivos Android escaneados (*software* instalado en 815 PCs y 2.275 smartphones y 821 *tablets* Android).

Ámbito: Península, Baleares y Canarias.

Diseño Muestral: Para cada CC.AA., estratificación proporcional por tipo de hábitat, con cuotas de segmento social y número de personas en el hogar.

Trabajo de Campo: El trabajo de campo ha sido realizado entre enero y junio de 2021 mediante entrevistas online a partir de un panel de usuarios de Internet.

Error Muestral: Asumiendo criterios de muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5, y para un nivel de confianza del 95,0%, se establece que al tamaño muestral n=3.711 le corresponde una estimación del error muestral igual a ±1,61%.

El informe *"Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España"* ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad (ONTSI):

Lucía Velasco
Alberto Urueña
Santiago Cadenas Villaverde

Agradecer la colaboración en la realización de este estudio a Hispasec y GfK

EDITA: Ministerio de Asuntos Económicos y Transformación Digital
Paseo de la Castellana, 162
28046 Madrid

NIPO: 094-21-113-5
DOI: 10.30923/ciu_ciberries_2021_2

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Twitter: @ONTSI
www.ontsi.es